

Security & Compliance Summary

SECURITY & COMPLIANCE SUMMARY

Posture, stated without ambiguity.

Written for an Information System Security Officer, an Authorizing Official, and a contracting officer reading in sequence. It states what we build to, what we hold, and what we do not hold, in that order, because the third item is the one most vendor documents omit.

Wagoner Enterprises, LLC. Founded May 2023. Bruce Wagoner, Chief Technology Officer. 202-794-3282. Washington, D.C. metro area.

AUTHORIZATION HELD

None

No ATO, no FedRAMP authorization, no provisional authorization

TECHNOLOGY READINESS

TRL 5 to TRL 6

By solution; PursuitIQ and Rostrum at TRL 6

CERTIFICATIONS HELD

None claimed

Status provided in writing on request

CUSTOMER DATA

Not retained

Not retained, not trained on, not accessed

SECTION 01

What we hold today, stated plainly.

This section exists so that nobody has to infer it from the rest of the document.

Authority to Operate

We do not hold one. No product in this portfolio carries an ATO, a FedRAMP authorization, a provisional authorization, or a DoD Impact Level accreditation. Products are engineered to the design discipline of a system on a path to authorization, which is a statement about engineering, not about a granted authority.

Management system certifications

We claim none. ISO 9001, ISO 27001, and CMMI are named on our Proof page as frameworks we work toward, with status provided in writing on request. Where the answer is that a certification is not held, that is the answer you will receive.

CMMC

Practices aligned. That is alignment, not certification. Current certification status is provided in writing on request.

Facility clearance

Facility clearance and cleared personnel status are provided on request. Nothing we publish should be read as a claim to hold a facility clearance.

Technology readiness

TRL 5 to TRL 6 by solution. PursuitIQ and Rostrum are TRL 6, demonstrated in a relevant environment on live federal pursuits; the remaining solutions are TRL 5, validated end to end in a relevant laboratory environment. All are delivered as containerized, Kubernetes-deployable workloads engineered to enterprise deployment standards. Production hardening, accreditation, and site-specific engineering are scoped per program.

Intellectual property

Patent pending. Wagoner Enterprises, LLC has filed United States patent applications covering technologies across the portfolio. No patent has yet issued. Application details are provided under appropriate agreements.

SECTION 02

Frameworks the engineering is built against.

Alignment means the control intent shaped the design and the product emits evidence mapped to it. It does not mean a third party has assessed us against it.

NIST SP 800-53 Rev. 5

Control baseline alignment for all deployments. Control mappings ship inside the Evidence Pack.

Aligned

NIST SP 800-37 Rev. 2

Aligned

Risk Management Framework process and evidence model.

NIST SP 800-207

Aligned

Zero Trust Architecture as the architectural foundation.

NIST SP 800-218 v1.1 (SSDF)

Aligned

Secure Software Development Framework practices in the delivery pipeline.

NIST SP 800-161 Rev. 1 (C-SCRM)

Aligned

Cybersecurity supply chain risk management, evidenced by SBOM and provenance.

NIST AI RMF 1.0 (NIST AI 100-1)

Aligned

AI risk management, evidenced by AI-BOM, model cards, and data cards.

OMB M-26-05

Tracked

Risk-based approach to software and hardware security, issued 23 January 2026, which rescinded the attestation common form set by M-22-18 and M-23-16 and left assurance requirements to each agency. Our outputs are designed to satisfy an agency-defined requirement rather than a single federal form.

Section 508 and WCAG 2.2 AA

Designed to

Accessibility is a procurement requirement. Interfaces are designed against it and an accessibility conformance report is produced per deployment.

A note on a commonly confused point. FedRAMP authorizes unclassified systems only. Classified operation is governed by the DoD Cloud Computing Security Requirements Guide at Impact Level 6 and by ICD 503 for intelligence community systems. There is no FedRAMP path to a classified authorization, and any vendor implying otherwise should be questioned.

Data handling and rights.

WHAT WE COMMIT TO

- ✓ You own your data. We do not retain it, train on it, or access it.
- ✓ The commitment covers operational data, prompts, logs, and telemetry, not just the primary dataset.
- ✓ Classification, source, and handling caveats are enforced at storage, at retrieval, and at display, not advisory labels.
- ✓ Tenants are logically isolated, with namespace or cluster level isolation available where required.
- ✓ A self-hosted, in-boundary inference mode is available so no model call leaves the authorization boundary.
- ✓ Licensing is structured for government use, with unlimited rights to program-specific deliverables produced under your task order.

WHAT YOU SHOULD VERIFY, NOT TAKE ON TRUST

- ✓ Ask for the contract clause, not the marketing sentence, on data retention and training.
- ✓ Ask which components make outbound calls in the tier you are buying, and confirm it against a network policy.
- ✓ Run the export during a pilot and confirm you can read it with tools you already own.
- ✓ Verify an Evidence Pack yourself using the three steps in our artifact specimens document.
- ✓ Request government-led testing, including independent assessment and source code review under agreement.

Deployment tiers.

The same artifacts deploy across tiers. What changes is the environment profile and the control overlay applied to it, not the architecture.

Connected

Commercial or government cloud. Managed services may be used on the inference path where the program authorizes them.

Disconnected

File-based ingestion and controlled export as the default operating mode. No SaaS dependency and no call-home requirement.

In boundary inference

Fully self-hosted speech, language, and vector stack. No external model calls of any kind.

Higher tiers

Pre-engineered, not accredited. Deployment above the tiers above is scoped per program and depends on the sponsoring authority.

What we will not say.

A short list, published because a buyer can use it to test us.

- ✓ We will not claim a certification we do not hold, or imply one by placing it in a list of things we do hold.
- ✓ We will not claim our tooling delivers, accelerates, or guarantees an ATO. It produces evidence that supports one.
- ✓ We will not publish a metric we cannot show you the methodology for.
- ✓ We will not name a customer without that customer's consent.
- ✓ We will not describe a product as fielded when it is a prototype.
- ✓ We will not mark a product as patented while the applications are pending.

If you find anything on our site or in our documents that breaks one of these, tell us and we will correct it. That is a standing offer, and it is easier to keep than to recover from.