

Responsible AI in Government Operations

Innovation should never come at the cost of security.

Dave Hoon
Chief Technology Officer, Norseman Defense Technologies · February 2026

AI is transforming government operations, but rapid adoption without strong safeguards risks exposing sensitive data.

At Norseman Defense Technologies, we help agencies deploy AI responsibly: secure-by-design, privacy-focused, and mission-ready. Innovation should never come at the cost of security.

What Responsible AI Deployment Requires

Moving fast on AI without a security foundation creates liabilities that are expensive to unwind. The agencies that get this right invest upfront in three things:

- **Secure-by-design architecture.** Security controls are embedded in the AI system from the start—not bolted on after the model is already running. This means data minimization at ingest, access controls matched to classification level, and audit logging built into every inference request.
- **Privacy-focused data handling.** For sensitive workloads, AI systems should never route data to commercial cloud providers. Private LLM deployments that operate entirely within the agency boundary are the standard for CUI and above.
- **Mission-ready governance.** AI systems need continuous monitoring, model validation against current threat intelligence, and clear escalation paths when confidence thresholds aren't met. A model that performed well at deployment can drift—governance ensures it stays mission-aligned.

The Risk of Moving Without a Foundation

The pressure to deploy AI quickly is real. But agencies that skip the security foundation end up with systems that create compliance gaps, generate unauditable decisions, or expose sensitive data through model outputs.

We've seen this pattern repeatedly in commercial deployments that moved into government environments without adjustment. The models weren't wrong—they just weren't built for the regulatory and operational reality of federal work.

Procurement Paths

AI infrastructure and deployment services are available through **ITES-4H**, **NASA SEWP V**, **NASA SEWP VI**, **GSA MAS**, and **CIO-CS**. SEWP VI ordering opens November 1, 2026, and SEWP V ordering is extended through January 31, 2027. Contact **Norseman** to discuss your agency's AI requirements.

Published at norseman.com/insights/responsible-ai-government-operations. To talk with Norseman Defense Technologies, call 410.579.8600 or email sales@norseman.com.