carahsoft

MANIFEST

AI Security for the FY '26 NDAA

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, ITES-SW2, Texas DIR TSO-4288 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Manifest, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/ManifestResources

Join Events & Webinars:
carah.io/ManifestEvents

Discover Technology Solutions:
carah.io/Manifest

Learn About Procurement:
carah.io/ManifestContracts

Connect With Our Team:
ManifestCyber@carahsoft.com
(703) 871-8548

MANIFEST

2026 Solution Brief

AI Security for the FY '26 NDAA

A comprehensive solution to address congressional mandates and close critical gaps

Executive Overview

The FY26 NDAA establishes lifecycle-based AI governance and supply-chain transparency for defense systems. However, critical gaps remain: no comprehensive AI inventory, no continuous dependency monitoring, and no AI-specific vulnerability processes. This framework translates NDAA policy into operational capability."

The Challenge

What the NDAA Mandates vs. What's Missing

NDAA REQUIREMENTS	IMPLEMENTATION GAP
Unified AI security policy across lifecycle	No inventory requirement of AI systems and training data in use
SBOM application to AI systems	No defined process for AI component tracking over time
Supply chain transparency	Inability to apply adversarial nation restriction without provenance data

Figure 1: Shadow AI can be shipped with any third-party software, including open-source. Internal teams can also be using shadow AI if there is not governance oversight.

Start managing your AI like a mission asset.

Contact us at info@manifestcyber.com to request a no-cost pilot.

The Solution

AI & Autonomous System Governance Platform

A comprehensive platform that operationalizes NDAA requirements through continuous discovery, policy enforcement, and transparency mechanisms purpose-built for AI systems.

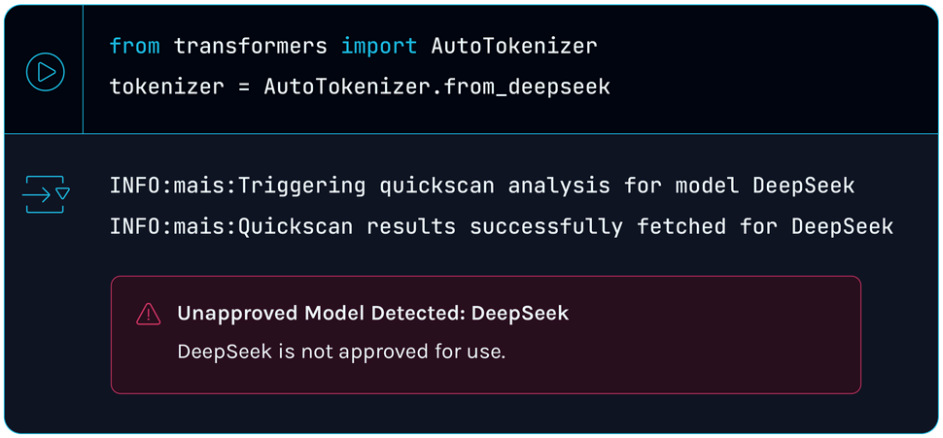

Figure 2: An example AI governance policy alert shown to a developer that tries to load an unsanctioned AI model.

Core Capabilities

Comprehensive AI Asset Discovery: Automatically inventory AI models, datasets, frameworks, and dependencies across development environments, CI/CD pipelines, notebooks, and production systems. Surface shadow AI and embedded models that bypass formal governance processes.

Risk-Based Policy Enforcement: Classify models as Approved, Restricted, or Forbidden based on configurable policies including country of origin, licensing terms, supplier trustworthiness, embedded software vulnerabilities, model maturity, and maintenance status.

Continuous Compliance Monitoring: Track model versions, dependency changes, and governance status over time. Automatically flag policy violations as models are retrained, weights updated, or datasets refreshed.

AIBOM & Risk Reporting: Generate machine-readable AI Bills of Materials capturing models, training data sources, software dependencies, and licensing. Produce risk summaries supporting internal reviews, acquisition decisions, ATO documentation, and NDAA transparency requirements,

Operational Benefits

- **For Chief AI Officers & CISOs:** Unified visibility into AI assets, automated risk assessment, and audit-ready documentation that scales with AI adoption velocity.
- **For Acquisition Leaders:** Vendor transparency requirements embedded in procurement workflows; enforceable security criteria that flow down to contractors.
- **For Mission Owners:** Confidence that AI systems meet security, licensing, and provenance standards without slowing mission delivery or innovation.
- **For Defense Contractors:** Clear path to AIBOM generation, policy compliance validation, and security posture demonstration required for DOD sales.

Policy Framework Implementation

Based on industry best practices, the solution implements a six-pillar policy framework that directly addresses both NDAA mandates and real-world AI supply-chain risks:

POLICY DOMAIN	WHAT IT DOES & WHY IT MATTERS
Country of Origin	Blocks models from sanctioned nations (China, Russia, Iran, DPRK). Enables adversarial nation compliance.
License Compliance	Identifies AI model licenses that introduce business risk.
Trusted Suppliers	Maintains approved/denied vendor lists with cryptographic verification. Implements supplier risk management.
Embedded Software Risk	Scans dependencies for CVEs and known exploits. Fulfills NDAA SBOM requirements for AI.
Model Maturity	Enforces 90-day public availability window. Risk-based lifecycle approach.
Maintenance Status	Requires active development within 12 months. Supports continuous monitoring.

Conclusion

The FY26 NDAA sets policy direction, but operational capability requires infrastructure. This framework transforms NDAA mandates into strategic advantages through automated discovery, governance, and transparency.