carahsoft

MANIFEST

Manifest Corporate Overview

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

CORPORATE OVERVIEW

Modern defense systems run on complex software and AI that are hard to see, track, and secure. Manifest gives national security teams a real-time, authoritative view of software and AI across their systems, showing where risk exists and how it spreads so they can act faster and respond to threats with confidence.

CORE COMPETENCIES

Enhance Mission Assurance
Manifest maps every software component and dependency to the exact asset where it runs, enabling precise mission-system risk decisions, continuous monitoring, and rapid remediation across fleets.

Field Tech Faster
Manifest accelerates ATO with automated software inventory, vulnerability management, and eMASS integration to keep POA&Ms current, collaborate with vendors, and maintain continuous visibility into operational dependencies.

Govern AI and Manage Risks
Manifest shows where models run, how they were built, and what they depend on, enabling informed approvals, clear use tracking, and early detection of dataset, licensing, and deployment risks before they hit mission systems.

PAST PERFORMANCE

Manifest is trusted by some of the world's largest and most critical national security organizations. Our flagship software supply chain security platform is used to secure the nation's critical assets.

END USERS

- SCRM & C-SCRM Teams
- DevSecOps
- Configuration Managers
- Acquisitions & ATO teams
- CIO & CDAO
- Incident Response, SOCs

OUR ACCREDITATIONS

FedRAMP · DOD Impact Level 5 · AWARDABLE {MP} PLATFORM ONE · SOC 2 TYPE 2 · GDPR · NIST 800-171 Compliant

CAPABILITIES & DIFFERENTIATORS

AI Bill of Materials (AIBOM) Generation
Enable R&E and Acquisition teams to assess AI model risks pre- and post-procurement, while governing model usage and compliance at enterprise scale.

CI/CD Integration & CLI
Automate analysis and monitoring through CI/CD pipelines, APIs, and CLI tools across the DevSecOps lifecycle.

Map Software to Hardware & Fleets
Link software components to hardware and fleet systems to understand risk at the asset level.

Reverse Engineer Binaries and Firmware
Generate SBOMS and component inventories from compiled binaries using reverse-engineering techniques when source code isn't available.

C/C++ SBOM Generation Support
Provides support for legacy languages commonly used in mission systems, often missed by standard tooling.

Automatic FOCI Risk Identification
Monitor open-source software (OSS) for contributors tied to adversarial nations and institution, enabling policy enforcement before software ships.

Continuous Monitoring & cATO
Know exactly how a new vulnerability impacts your fleet as soon as it is identified, across platforms, systems, and deployments.

Deployment Options & FedRAMP HIGH
Supports IL-5 SaaS deployments, as well as on-premises and air-gapped environments, to securely support higher classifications.

ABOUT THE MANIFEST PLATFORM

Government agencies increasingly depend on third-party software and AI, yet often lack clear, end-to-end visibility into what's embedded across mission systems. That blind spot allows vulnerabilities and compliance gaps to persist—driving up security, audit, and operational risk. Strong risk management starts with comprehensive visibility and continuous assessment of all software, whether developed internally or acquired externally. The Manifest Platform centralizes this visibility and continuously identifies risk across software, AI, and suppliers to help agencies protect mission outcomes.

- Product Security – Gain a live, prioritized view of vulnerable components in your software, enabling faster response and more efficient remediation.
- AI Risk – Monitor and govern the use of generative AI models and data, enforcing responsible AI practices while reducing hidden risks.
- Supplier Risk – Achieve continuous visibility into third-party software and vendors, uncovering risks across the entire supplier lifecycle.

TECHNICAL DETAILS

SUPPORTED IMPORT METHODS

Import SBOM:
- CycloneDX
- SPDX
- CSAF or OpenVEX

Import OSS:
- GitHub
- GitLab
- BitBucket

Import AI Model:
- Hugging Face
- Binary Analysis
- SCA

SUPPORTED LANGUAGES AND FRAMEWORKS

- Alpine
- C
- C++
- Dart
- Debian
- Elixir
- Erlang
- Go
- Haskell
- Java
- JavaScript
- Jenkins plugins
- .NET
- Nix
- PHP
- Python
- Red Hat
- Ruby
- Rust
- Swift
- Others

API

Use Cases:
- SIEMs
- Ticketing Systems
- Vulnerability Scanners
- Assest Management
- Messaging Systems

INTEGRATIONS

- GitHub
- GitLab
- BitBucket
- JIRA
- ServiceNow
- Linear