CASE STUDY

U.S. GOVERNMENT · DEFENSE INDUSTRIAL BASE

USE CASE · SUPPLY CHAIN RISK MANAGEMENT

Federal Defense Agency

Source-linked FOCI screening for missile defense supply chain risk – selected over alternatives that could not provide original-source evidence.

<10

PERSONNEL COVERING SCRM MISSION

For all of the agency's programs

40+

HOURS OF TECHNICAL VALIDATION CALLS

Validating API integration with custom GOTS algorithm

0

FOCI ILLUMINATION DATA

In the existing system before deployment

01 AT A GLANCE

CHALLENGE

No FOCI or sub-tier supplier illumination data in the system

The agency had deployed complementary tools for cyber risk and operational risk, but no tool filled the FOCI and ownership intelligence gap essential for the mission.

SOLUTION

Full data provenance - government buyers rejected black-box alternatives

The champion logged 40+ hours of technical calls validating that the platform's API could feed the agency's custom GOTS risk scoring algorithm. Competing solutions were rejected specifically because they could not provide source-linked evidence.

RESULT

Mission-aligned FOCI data layer powering the agency's risk dashboard

Full platform deployment: API feeds, investigative tools, and supply chain mapping powering the stoplight risk dashboard with the most authoritative FOCI data available.

02 THE CHALLENGE

A data gap in a classified defense supply chain – and no source Congress would trust

Supply chain risk management is now a national security imperative. The DoD published its first coordinated SCRM Taxonomy and a new SCRM Guidebook, and stood up the SCRM Integration Center under USD(A&S), tasked with identifying and mitigating supply chain risks across the defense industrial base. For agencies responsible for the most sensitive weapons programs in the U.S. arsenal, adversaries exploit opaque corporate structures to embed foreign influence within the defense supply chain.

The agency's Quality, Safety, and Mission Assurance office was screening aerospace and defense suppliers for counterintelligence threats, foreign influence, and solvency risk. The team was small - fewer than 10 people - but responsible for supply chain risk assessments across all of the agency's programs. The critical gap: no FOCI and sub-tier supplier illumination data existed in their system.

KEY POINTS

- Team of fewer than 10 responsible for supply chain risk assessments across all programs
- No FOCI and sub-tier supplier illumination data in the existing system
- Cyber risk and operational risk had tools - the FOCI gap remained unfilled
- Mission requires source-linked evidence for senior leadership and interagency briefings

Primary-source FOCI data feeding a Government-Owned scoring application

The engagement began through a DoD CIO pilot program, where the agency was one of the first to request hands-on access. The champion, a PhD-level SCRM expert in the agency's mission assurance office, logged over 40 hours of technical calls to validate that the platform's API could feed the agency's custom GOTS risk scoring algorithm.

The key differentiator: full data provenance. Government buyers explicitly rejected "black box" tools. They needed data with original source documentation that could support senior leadership and interagency briefings. Competing solutions were rejected specifically because they could not provide source-linked evidence. The agency ultimately determined that selecting any other source would result in substantial duplication of cost and unacceptable delays.

KEY POINTS

- DoD CIO pilot program - agency was one of the first to request hands-on access
- PhD-level SCRM champion logged 40+ hours of technical calls validating GOTS integration
- Black-box alternatives rejected - full data provenance required for briefing-ready intelligence

SAYARI CAPABILITIES USED

Sayari Graph | Supply Chain Mapping | API Integration | FOCI Screening | Sub-Tier Illumination | Source-Linked Evidence

The only FOCI intelligence layer. Full-stack deployment. Congressional-grade evidence.

The agency operates with a capability that did not exist before: automated, source-linked FOCI screening integrated directly into its mission-owned risk platform. Mission owners get clear risk signals. Analysts get investigative depth. Leadership gets briefing-ready intelligence backed by original source documents, not opaque algorithms.

<10	40+	Stoplight
Personnel covering the agency's SCRM mission	Hours of technical validation against the GOTS risk-scoring algorithm	Risk dashboard backed by source-linked evidence

> *"Selecting any other source would result in substantial duplication of cost and unacceptable delays."*
>
> SCRM LEAD, FEDERAL DEFENSE AGENCY

READY TO ACT ON WHAT YOU FIND

Ready to see *your data*?

Sayari is the judgment infrastructure for trustworthy AI in economic security and commercial risk, built on the world's most comprehensive commercial knowledge graph.

Request a Demo →

sayari.com/demo/

SAYARI