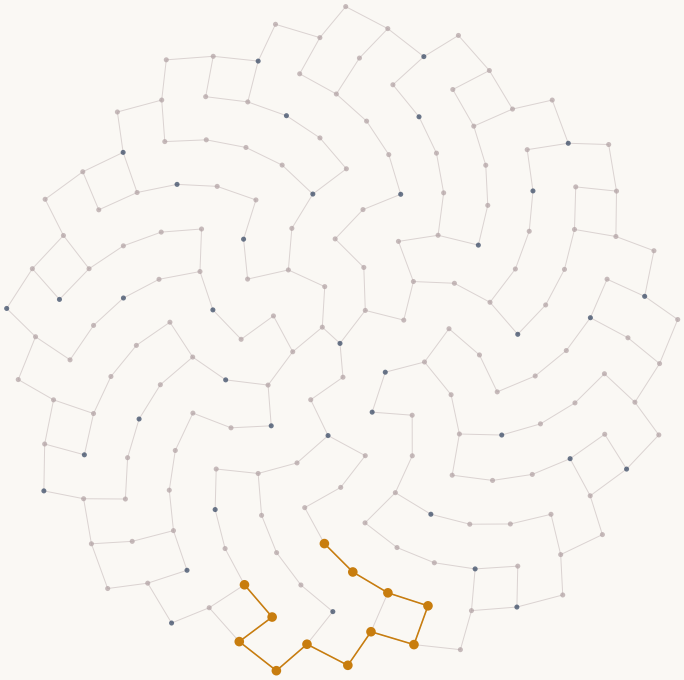
A SAYARI GOVERNMENT / SUPPLY CHAIN BLOG . MAY 2025 . SAYARI ANALYST TEAM



DoD SCRM Taxonomy v2.1: What the Update Means for Contractors

The DoD's updated SCRM framework expands supply chain risk beyond watchlists.

Here's what changed and why it matters.

By Sayari Analyst Team . Published May 2025 . sayari.com

GOVERNMENT / SUPPLY CHAIN

DoD SCRM Taxonomy v2.1: What the Update Means for Contractors

By Sayari Analyst Team · Published May 2025

The DoD's updated SCRM framework expands supply chain risk beyond watchlists. Here's what changed and why it matters.

For years, many defense contractors operated under a narrow assumption: supply chain risk management meant maintaining compliance with watchlist screening-checking names against the BIS Entity List, OFAC sanctions lists, and debarment databases. This approach worked when the threat landscape was simpler. But the Defense Department's Supply Chain Risk Management (SCRM) Taxonomy v2.1, released in March 2025, formalizes a reality that has been quietly reshaping defense procurement: watchlist screening is necessary but insufficient. The updated taxonomy defines a multi-dimensional risk framework that spans regulatory compliance, manufacturing capacity, foreign ownership and control, political exposure, financial stability, product integrity, and infrastructure resilience. For contractors accustomed to point-in-time name checks, this represents a fundamental shift toward continuous, multi-factor risk assessment across the entire supply chain ecosystem.

What Changed in SCRM Taxonomy v2.1

The original SCRM Taxonomy, introduced in late 2022, provided the first formal DoD structure for categorizing supply chain threats. Version 2.1 builds on that foundation with three critical improvements: increased granularity in risk definitions, reduced redundancy in category overlap, and explicit incorporation of contractor and supplier feedback gathered over two years of operational use. The update maintains the DoD's commitment to standardizing how defense organizations identify, assess, and monitor supply chain vulnerabilities. For procurement officers and supply chain managers, this means clearer risk definitions, fewer gray zones between categories, and a framework that better aligns with actual procurement workflows. Rather than navigating conflicting interpretations of what constitutes FOCI risk or financial instability, the clarified taxonomy reduces ambiguity in risk categorization decisions. The timing matters: as geopolitical instability reshapes manufacturing networks, supply chain fragmentation accelerates, and foreign investment scrutiny intensifies at the government and board level, a clarified taxonomy helps contractors make faster, more defensible decisions about which suppliers and partners present acceptable risk profiles. Contractors face real deadline pressure during source selection and contract award-the framework must enable decisiveness without sacrificing rigor.

Seven Risk Categories and Why the Update Matters

FOCI-Foreign Ownership, Control, or Influence-emerges as particularly significant in the updated framework. This category extends far beyond simple country-of-origin questions. FOCI risk encompasses foreign intelligence entity (FIE) relationships, cross-border merger and acquisition activity that shifts control to foreign nationals, state-owned enterprises (SOEs) operating under government directives, nationalization actions that retroactively place assets under hostile government control, and veiled corporate structures designed to obscure actual ownership. A supplier might pass every watchlist check while remaining vulnerable to FOCI risk through a recent acquisition by a foreign government, a partial equity stake by a state-owned competitor, or operational control by individuals with ties to foreign intelligence services. Traditional name-based screening simply cannot surface these ownership and control relationships. Contractors need visibility into beneficial ownership chains, institutional investor profiles, and cross-border capital flows to assess FOCI exposure accurately.

The taxonomy's seven risk categories establish a more complete operational map. Regulatory & Compliance covers suspension and debarment status, contractor misconduct findings, procurement and government fraud charges, import/export violations, SEC enforcement

actions, conflict minerals traceability, human rights violations, and trafficking findings. This category matters because regulatory history reveals behavior patterns; a contractor with prior export control violations demonstrates systemic compliance deficiency, not a one-time lapse. Manufacturing & Supply encompasses production capacity constraints, single-source over-reliance, and supply chain concentration vulnerabilities. A supplier may be financially healthy and fully compliant but operate a single facility producing a critical component with no redundancy-a single geopolitical disruption, natural disaster, or cyber incident can halt production across your entire program. Geographic concentration in high-risk regions amplifies this vulnerability. FOCI-as noted-addresses foreign ownership, control, and influence pathways. Political risk includes exposure to sanctioned jurisdictions, politically exposed persons (PEPs), and destabilization activity, extending beyond simple country-of-origin questions to include board-level relationships and institutional investor exposure. Financial risk spans operational efficiency concerns, liquidity pressures, insolvency indicators, bankruptcy filings, and over-reliance on defense contracts as primary revenue-a supplier dependent on government work for 80% of revenue faces existential pressure if a contract terminates or delays. Product Quality & Design addresses counterfeit component infiltration and non-standard goods entering the supply chain, a particular concern in electronics-heavy defense manufacturing where component substitution can degrade performance or introduce backdoors. Infrastructure risk flags facility availability threats, cyber vulnerabilities, and operational continuity concerns. This architecture forces procurement teams to ask questions beyond "Is this supplier on a list?" Instead, the framework demands continuous assessment: Is this supplier financially stable? Is control shifting to a foreign entity? Are manufacturing bottlenecks emerging in my supply base? Does their operational infrastructure create single points of failure?

How the Framework Changes Contractor Obligations

The path forward demands a shift from reactive watchlist compliance to proactive, data-driven risk monitoring. Contractors cannot manually track 200+ risk factors across thousands of suppliers, validate news alerts against false positives, monitor financial distress indicators in real time, or surface beneficial ownership changes before they create compliance exposure. The SCRM Taxonomy v2.1 provides the framework; execution requires infrastructure. Risk management platforms now need to integrate regulatory data, financial filings, adverse media monitoring, corporate registry information, and sanctions list updates into a unified assessment engine. This is where platforms like Sayari's defense intelligence solutions become operational necessities. Sayari ingests more than 200 core risk factors-regulatory status, financial indicators, ownership changes, adverse news, and FOCI signals-and flags entities controlled by parties sanctioned by the U.S., EU, UK, Australia, Japan, and Ukraine. Real-time monitoring surfaces risk changes as they occur, replacing point-in-time snapshots with continuous visibility. For a defense contractor managing a supply base of hundreds or thousands of entities, this level of automation transforms compliance from a quarterly checkbox exercise into a genuinely embedded operational control.

From Taxonomy to Practice: Implementing SCRM in the Defense Supply Base

The DoD SCRM Taxonomy v2.1 represents the formal acknowledgment that supply chain risk is structural, continuous, and multi-dimensional. Contractors who treat it as an expanded checklist-adding FOCI questions to watchlist screening-will improve their risk posture incrementally. Those who integrate the taxonomy into procurement workflows, vendor onboarding processes, and continuous monitoring protocols will build genuine resilience. If your organization is still relying primarily on watchlist screening, now is the moment to reassess. Learn how Sayari's defense intelligence platform maps the complete SCRM risk landscape for defense contractors and procurement teams. Request a demo to see how real-time risk monitoring aligns with DoD SCRM Taxonomy v2.1 requirements and moves your organization beyond compliance toward proactive supply chain resilience.

Please visit sayari.com to learn more.