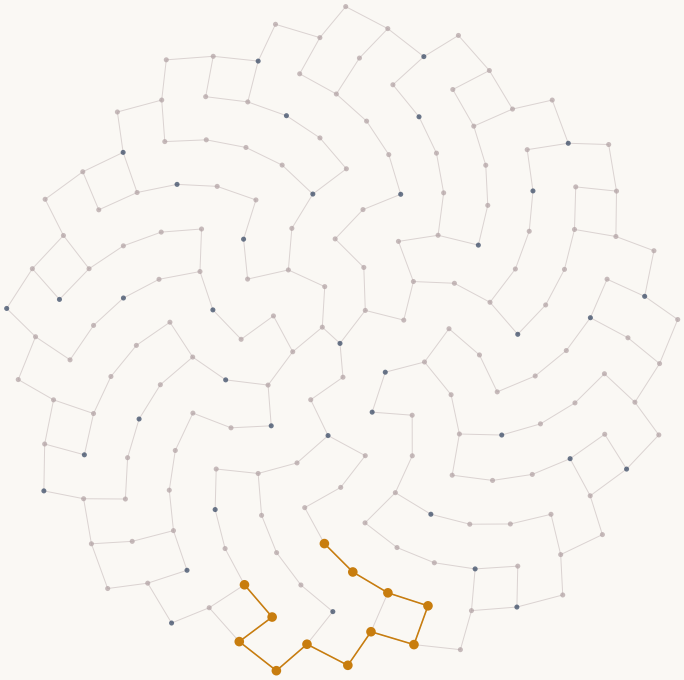

Are Defense Supply Chains Over-Reliant on Foreign Adversaries?

The Department of Defense manages procurement across 200,000+ suppliers globally, yet most federal agencies lack visibility into critical lower-tier dependencies on Chinese and Russian entities.

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

GOVERNMENT / SUPPLY CHAIN

Are Defense Supply Chains Over-Reliant on Foreign Adversaries?

By Sayari Analyst Team · Published May 2025

The Department of Defense manages procurement across 200,000+ suppliers globally, yet most federal agencies lack visibility into critical lower-tier dependencies on Chinese and Russian entities.

Procurement teams once assumed domestic prime contractors provided adequate supply chain security. But the COVID-19 pandemic and post-Ukraine audits exposed a structural illusion: beneath first-tier vendor relationships lay complex dependencies on foreign suppliers-some in designated adversary nations. These lower-tier relationships remained invisible to federal agencies responsible for national security.

The Department of Defense relies on more than 200,000 suppliers worldwide delivering everything from guided missiles to military vehicle batteries to advanced manufacturing equipment. The post-Ukraine environment elevated supply chain resilience from logistics concern to strategic imperative. Yet institutions defending the nation still lack comprehensive visibility into who supplies their suppliers-and whether those suppliers answer to foreign intelligence services. This gap between perceived and actual control defines the current moment in defense industrial policy.

The Scale of the Problem: An Opaque Network Under Scrutiny

The DoD's supplier network makes comprehensive oversight impossible under legacy processes. When the Global Supply Chain Institute at Michigan State University analyzed modern supply chain complexity, researchers found defense manufacturers depending on networks spanning dozens of countries and hundreds of layers below prime contractor tier.

The 2022 CHIPS and Science Act directed $280 billion toward U.S. semiconductor manufacturing, recognizing chip dependencies as critical vulnerabilities. The 2021

Infrastructure Investment and Jobs Act allocated billions toward domestic manufacturing. These represented strategic recognition that globalized, cost-optimized supply chains created failure points adversaries could exploit.

In July 2025, the Government Accountability Office released "Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers." DoD still has limited lower-tier supplier visibility despite years of transparency initiatives. Mapping remains incomplete, data sharing fragmented, and visibility below second or third tier largely unavailable. COVID-era disruptions illuminated this blindness. When polyimide film production concentrated in Japan faced lockdowns, U.S. advanced electronics manufacturers suddenly lacked critical inputs. These immediate crises disrupting defense system production raised inevitable questions: if a pandemic exposed these dependencies, what would an adversary with intent accomplish?

Why Visibility Remains Elusive: Data Silos and Shifting Priorities

Building n-tier supply chain visibility requires overcoming structural obstacles. Supplier data exists in fragmented systems held by different agencies, contractors, and subcontractors with minimal incentive to share. Prime contractors treat supplier relationships as proprietary competitive advantages rather than national security assets. Federal procurement historically optimized for cost and speed, not security. Procurement systems found lowest-cost bidders, not traced ownership chains through shell companies or identified hidden foreign stakes in ostensibly domestic firms.

National Defense Authorization Act amendments began shifting incentive structures, requiring deeper scrutiny for foreign intelligence and state-owned enterprise ties. But changing rules is simpler than changing implementation systems. Legacy procurement databases weren't designed to ingest ownership-chain data. Integration between the Defense Counterintelligence and Security Agency, State Department, and Commerce Department remains limited.

Political and business complexity compounds this. Many U.S. corporations invested years in lower-cost supplier relationships. Requiring visibility and potentially demanding diversification or nearshoring carries real financial consequences. Foreign suppliers resist disclosure. The federal government historically lacked technical and legal infrastructure to demand transparency.

The New Legislative Framework: Toward Systematic Mapping

Congress began building infrastructure through the "Promoting Resilient Supply Chains Act of 2025," formalizing resilience efforts within the Department of Commerce through a Supply Chain Resilience Working Group. The working group maps, assesses, and models critical supply chains across the defense industrial base and other vital sectors, identifying gaps and vulnerabilities in semiconductors, rare earth minerals, batteries, pharmaceuticals, and advanced manufacturing.

The approach distinguishes itself through scope and technology integration. The working group is explicitly authorized to access data from multiple federal agencies, state governments, and industry partners, issue information requests to federal procurement companies, and develop shared databases and assessment tools. For the first time, legal frameworks authorize systematic defense supply chain ecosystem visibility. The act establishes public reporting standards: the working group must produce annual reports identifying critical vulnerabilities and recommending mitigation strategies. This transparency creates accountability and drives investment toward most critical vulnerabilities.

Executing Visibility: Technology and Implementation

Solving visibility requires technology tracking ownership and control chains through multiple layers, jurisdictions, and time. External trade data is critical: when companies trade internationally, transactions are recorded in customs data, bills of lading, and shipping registries. Integrating data from 78 international sources-customs records, business registries, shipping data, financial records, and regulatory filings-constructs comprehensive maps of trading relationships, entity control, and beneficial ownership locations. This bypasses voluntary disclosure limitations. If suppliers claim no Chinese investment but trade data shows regular state-owned enterprise shipments, discrepancies are immediate and verifiable.

This methodology traces ownership through multiple intermediary and shell company layers. Layered visibility-n-tier visibility-is now within reach for the defense industrial base. Agencies can map direct suppliers and suppliers to suppliers, identifying foreign adversary control in networks.

Evidence overturned the assumption that domestic prime contractors automatically provide supply chain security. The defense industrial base remains vulnerable to adversary leverage at multiple tiers below prime contracting. Legislative frameworks are in place. Institutional machinery is being built. Technology to map networks exists and improves continuously. What remains is execution: integrating technology into federal procurement processes, training analysts interpreting visibility data, and deciding which vulnerabilities warrant investment.

To learn more about defense and foreign ownership control requirements and gain greater visibility into complex supply chain dependencies, visit our defense intelligence resources or explore our sourcing and procurement solutions. Request a demo with our team to discuss your supply chain challenges.

Additional resources include the GAO Report "Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers" (July 2025), the CHIPS and Science Act of 2022, the Infrastructure Investment and Jobs Act of 2021, and the Promoting Resilient Supply Chains Act of 2025 (Senate Bill).

Please visit sayari.com to learn more.

This blog is for informational purposes and isn't intended to be legal advice.