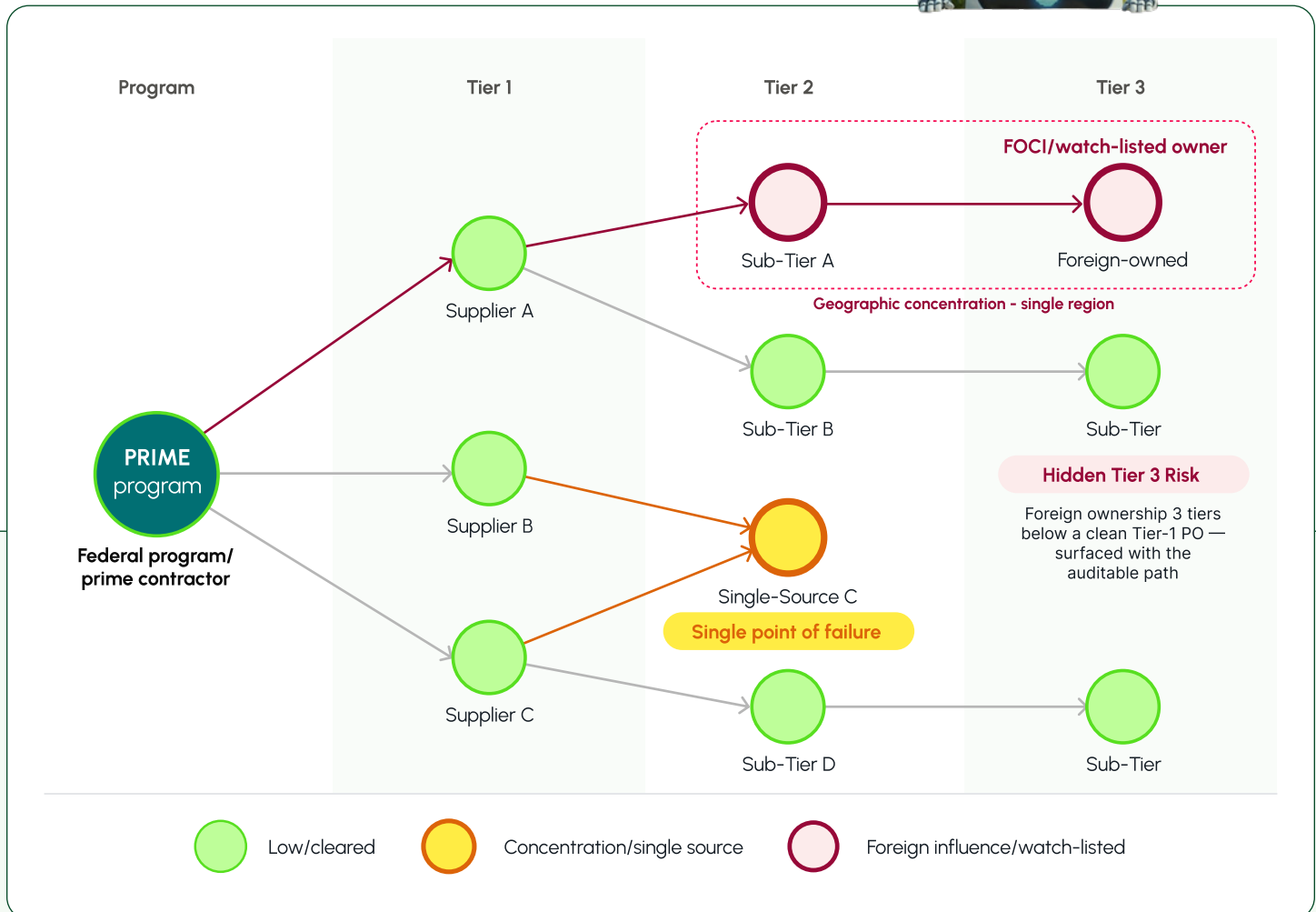


From Blind Spots to Full Supply-Chain Visibility

Federal supply chains span thousands of suppliers across tiers, geographies, and ownership structures — and the risk hides below Tier-1: foreign ownership and control, single-source dependencies, geographic concentration, counterfeit parts, and cascading disruption. Arango models the entire supplier network as one governed knowledge graph, so risk that traditional systems can't see becomes visible and auditable.

One purchase order sees Tier-1.
The graph reveals the risk buried tiers below.



One governed platform: Multi-tier visibility, foreign-influence detection, and disruption modeling for defense, logistics, and civilian agencies.

How Arango Manages Supply-Chain Risk



Six capabilities give federal supply-chain teams visibility, risk detection, and disruption modeling across every tier of the network.

Multi-Tier Illumination

Traverse supplier and ownership relationships from Tier-1 to Tier-N in a single query, with SmartGraphs keeping traversals fast at scale.

Entity Resolution

Resolve suppliers, subsidiaries, aliases, and identifiers scattered across systems into one authoritative entity.

FOCI & Transitive Risk

Follow ownership and control across hops to surface ties to foreign-owned or sanctioned entities, with an auditable path and risk score.

Concentration Detection

Reveal single points of failure and geographic concentration across the network before they cause an outage.

Disruption Modeling

Model an event (a port closure, supplier loss, or geopolitical shock) and trace second- and third-order impact to programs.

Hidden-Link Prediction

Use GraphSAGE and the Graph Analytics Engine to surface relationships that should exist but don't, and risky access paths that shouldn't.



Aligned to Federal Missions & Accounts



Defense & Aerospace

Illuminate tier-3 foreign influence (FOCI / CFIUS), model program impact, and trace parts provenance, feeding a model-based digital thread across the product lifecycle.



Logistics & Postal

Map the supplier, transporter, and facility network to find deployment hotspots, rebalance assets, and respond to disruption across a national operation.



Federal Civilian & ICT

Support C-SCRM and vendor illumination (NIST 800-161, Section 889), surfacing prohibited sources and counterfeit-parts risk across the ICT supply chain.

What Arango Gives Federal Supply-Chain Teams

Graph, vector, geospatial, search, and machine learning share a single query language and one governance model, giving supply-chain teams a complete, auditable view of risk across every tier.

Illuminate Every Tier

Traverse Tier-N supplier and ownership relationships in one query, not a chain of manual lookups.

Detect Foreign Influence

Surface FOCI, sanctioned, and watch-listed ties, each with the auditable path that produced the finding.

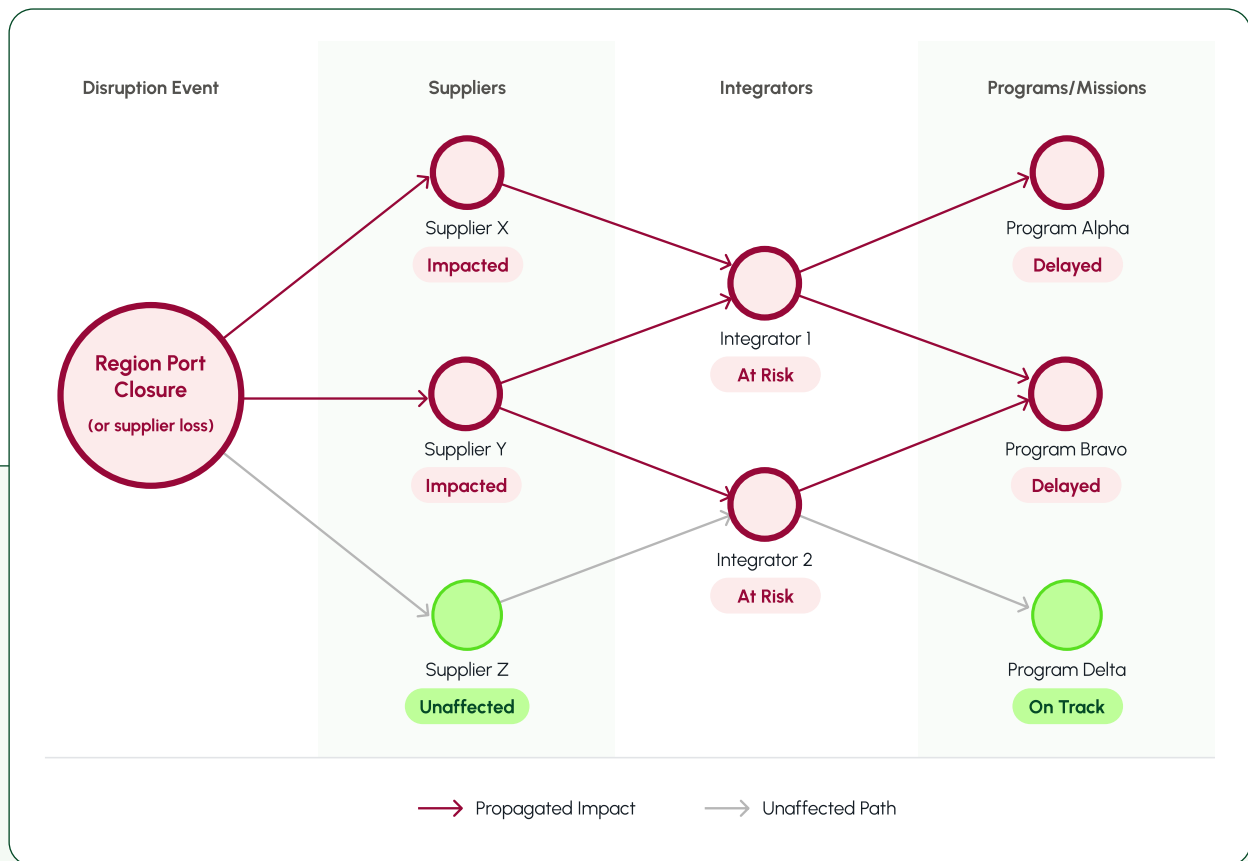
Model Disruption

Trace the blast radius of an event to the programs and missions actually affected.

From Tier-1 to a Defensible Risk Finding



Model a Disruption Once. Trace the Blast Radius.



A relational report shows the direct supplier. The graph traverses dependencies across tiers and geography to reveal the second- and third-order impact — which programs slip, by how much, and where to pre-position mitigation — as one query over the live network. Programs Alpha & Bravo are two contracts removed from the event and still exposed.

Platform Context

Supply Chain Risk Management runs on the same Arango Contextual Data Platform as Intelligence Analysis and Zero Trust. Graph, vector, geospatial, document, key-value, and search operate in one engine under a single AQL query, so supplier, ownership, and program data live in one governed graph instead of a chain of siloed systems that can't be traversed together.

Operational Impact

SmartGraphs shard the network by region or program, so multi-hop, multi-tier traversals stay fast as the graph grows to millions of entities, keeping risk analysis usable at national scale.



Built for Federal Supply-Chain Missions



Arango supports the federal SCRM drivers agencies must meet, while giving teams one platform built for national scale.



One Platform, Not a Frankenstack

Graph, vector, geospatial, document, key-value, and search in one engine — one query spans them all.



Built for National Scale

SmartGraphs shard the network by region or program, keeping traversals fast as the graph grows.



Secure & Sovereign by Design

Self-managed, on-premises, air-gapped, and distributed deployment keep control of sensitive supplier data.



Trusted & Auditable

Lineage, field-level access control, and immutable audit make every risk finding traceable to source.

Aligned to Federal Mandates

NIST SP 800-161 (C-SCRM)

Section 889 (NDAA)

EO 14017 (Supply-Chain Resilience)

FOCI / CFIUS

CMMC / DFARS

Trusted by These Organizations and Many Others



Ready to see the risk hiding three tiers below Tier-1?

Schedule a demo and trace your own supply chain's hidden dependencies and foreign-ownership risk.

arango.ai

federal@arangodb.com

