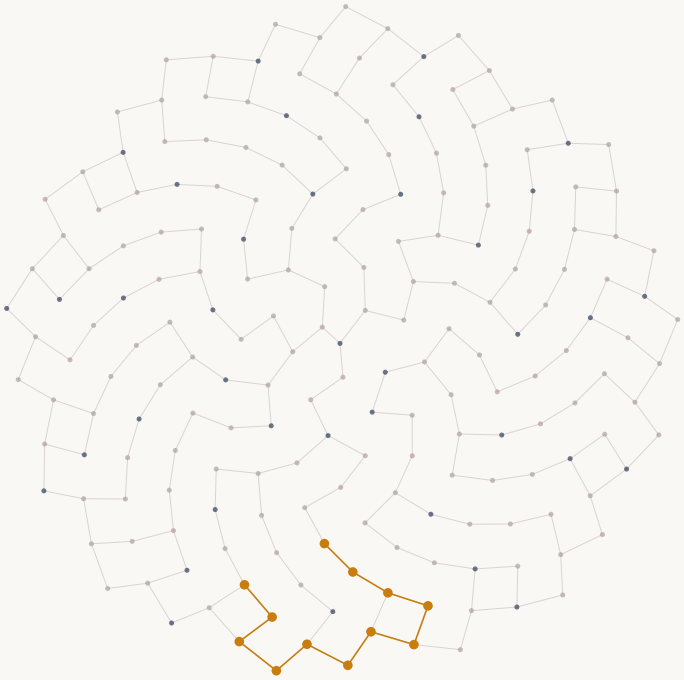

Aerospace & Defense Compliance in 2025: Supply Chain Security

Protecting defense supply chains from state-sponsored actors and product diversion requires mapping beyond tier-1 vendors to hidden ownership and transshipment networks.

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

AEROSPACE & DEFENSE

Aerospace & Defense Compliance in 2025: Supply Chain Security

By Sayari Analyst Team · Published April 2025

Protecting defense supply chains from state-sponsored actors and product diversion requires mapping beyond tier-1 vendors to hidden ownership and transshipment networks.

Most aerospace and defense compliance programs rely on watchlist screening against the Treasury Department's Consolidated Sanctions List and the Commerce Department's Entity List, with tier-1 vendor vetting. But if you've only screened direct suppliers, your supply chain is not secure. The real threat comes from suppliers' suppliers and hidden ownership structures that state-sponsored actors have woven into your extended network.

Boeing's 737 supply chain includes approximately 700 suppliers manufacturing roughly 2 million parts. Suppliers source from unauthorized distributors. Parts are diverted through transshipment networks. Foreign investors with undisclosed government ties acquire stakes in critical suppliers. The defense apparatus depends on secure access across more than 100,000 defense industrial base companies-too vast and opaque for traditional vetting.

The FY2026 National Defense Authorization Act amendments now require additional scrutiny of government contractors for ties to foreign governments. Meeting that requirement demands mapping ownership structures in opaque jurisdictions, connecting trade data to beneficial ownership, and identifying relationships compliance teams miss.

The Complexity of Modern Defense Supply Networks

Boeing's 700-supplier footprint is typical for modern defense primes. Each supplier has its own supply chain, foreign operations, and exposure to adversary-controlled entities. The Department of Defense faces a supply network too vast and opaque for traditional vetting to secure.

The FY2026 NDAA amendments make scrutiny for foreign government ties a compliance requirement-not a suggestion. Contractors must document diligence, showing evidence they have inquired into beneficial ownership of suppliers and investors. They must demonstrate coverage of nations with greatest opacity-China, Russia, Turkey-where ownership concealment is routine and state-sponsored acquisition is documented.

Supply chain officers need visibility into who owns suppliers, who owns their investors, and what connections those entities maintain to foreign governments. Validating vendor work and filling gaps requires resources and tools most companies lack.

Product Diversion and the Dual-Use Goods Challenge

Dual-use goods present persistent threat to supply chain security. Dual-use products-specialized electronics, precision bearings, advanced composites, semiconductor components-can be diverted from legitimate defense programs to unauthorized ends: conflict zones, sanctioned nations, or military programs of state-sponsored actors.

Diversion mechanisms are well understood but difficult to detect. A supplier receives an order from a distributor not on any watchlist. The order appears routine, but the distributor is a cut-out obscuring the actual end-user. Goods travel through transshipment points in third countries, are repackaged, documentation altered. Supply chain visibility evaporates.

Your compliance program must extend beyond the moment of sale to immediate customers. You must identify anomalous patterns in distributor orders-unusual geographic destinations, quantities, or timing. Most A&D; companies still lack systematic mechanisms to monitor for diversion or maintain continuous visibility into downstream distribution. Partnership with suppliers, distributor disclosure requirements, and collaboration with law enforcement are necessary.

Hidden Ownership and the Foreign Investment Threat

Acquisition of A&D; suppliers by foreign state-sponsored entities-structured to conceal true ownership-represents significant supply chain compromise risk. This is known as Foreign Ownership, Control, or Influence (FOCI). FOCI risk has accelerated as authoritarian governments acquire defense suppliers through intermediaries and investment vehicles that obscure government backing.

A foreign government actor establishes holding companies in opaque jurisdictions. An investment firm nominally controlled by private investors acquires a stake in your supplier. The hidden beneficial owner is a foreign intelligence service or defense ministry. Owners embed themselves in governance or technical operations, gaining access to intellectual property-engine components, sensor systems, communications protocols. They may redirect production to unauthorized customers or gain advance knowledge of U.S. defense capabilities.

A comprehensive FOCI assessment requires mapping the beneficial ownership chain several layers deep. You cannot rely on investor disclosures alone. You need to understand who owns the investors, their connections to foreign governments, what other companies they control, and their patterns of investment behavior. This requires investigation of corporate records in opaque jurisdictions, cross-referencing with intelligence on foreign government entities, and identifying networks of related companies. Most A&D; companies lack in-house expertise for this deep ownership diligence.

Going Beyond Watchlists: Toward Comprehensive Supply Chain Visibility

Watchlist screening against the Consolidated Sanctions List and the BIS Entity List catches some threats but cannot catch hidden ownership, diversion patterns, or networks across opaque jurisdictions. The path forward requires connecting transactional data to beneficial ownership data to identify relationships watchlists cannot reveal. Combine trade data with ownership registries, apply network analysis to identify connections, maintain coverage in China, Russia, Turkey-where opacity is greatest-and develop the intelligence foundation to detect supply chain compromises.

This means moving beyond periodic audits to continuous monitoring. It means integrating supplier screening into procurement workflows before vendors join your supply network. It

means establishing feedback loops with suppliers to identify concerning ownership changes or transshipment anomalies. And it means partnering with specialized intelligence providers who maintain current knowledge of beneficial ownership in opaque jurisdictions.

The FY2026 NDAA amendments signal zero tolerance for hidden foreign government ties in defense supply chains. Companies that wait to be forced into deeper diligence will find themselves at disadvantage. Supplier screening and procurement intelligence is becoming fundamental to A&D; operations.

If your program relies primarily on watchlist screening and annual audits, you are operating with an outdated risk model. The threats-product diversion, hidden foreign ownership, sub-tier compromise-are real and documented. Intelligence-driven supplier screening is reshaping A&D; supply chain security. We encourage you to request a demonstration of how comprehensive ownership visibility can strengthen your compliance posture.

Please visit sayari.com to learn more.

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