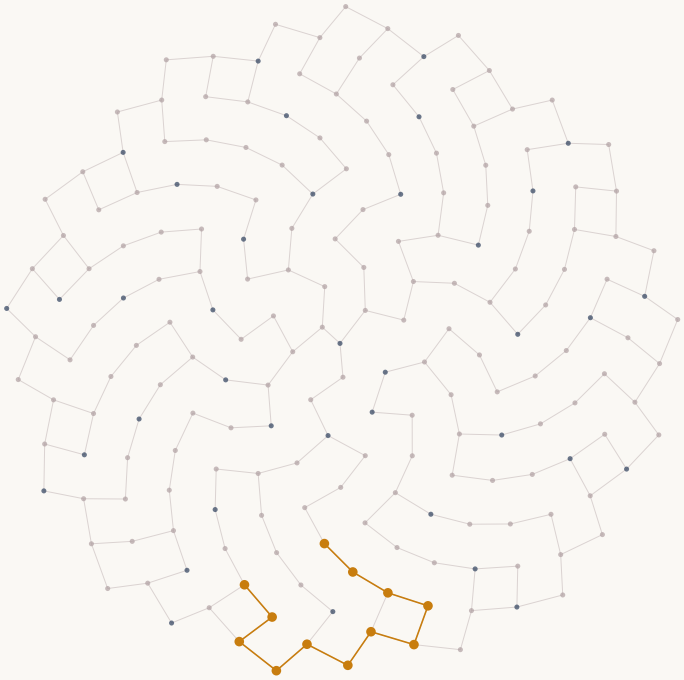

Tech & Electronics Compliance 2025: Export Controls

Electronics compliance programs must move beyond list-based screening to address parent-company export controls, supply-chain forced labor, and semiconductor diversion risk to restricted military entities.

SUPPLY CHAIN

Tech & Electronics Compliance 2025: Export Controls

By Sayari Analyst Team · Published April 2025

Electronics compliance programs must move beyond list-based screening to address parent-company export controls, supply-chain forced labor, and semiconductor diversion risk to restricted military entities.

Your compliance team runs daily screenings against the BIS Entity List and OFAC SDN lists. You flag every match and believe you're covered. But in 2025, this assumption is broken. Compliance risk in electronics and semiconductors extends far beyond list-based screening.

Export controls now require understanding parent-company nationality and operational proximity to military facilities. Forced labor risks hide in sub-tier suppliers-electronics imports face the highest forced labor risk across G20 nations at $243.6 billion in imports. Semiconductor diversion, where civilian-grade chips flow to restricted military end-users through intermediaries, operates through supply chains that no static list can capture. These gaps expose your organization to enforcement action, reputational damage, and supply-chain disruption.

The regulatory landscape has shifted fundamentally. Export controls no longer depend solely on direct listing. Ownership structures, facilities co-location, and Material Change of Circumstances (MCC) connections create liability even when a party avoids formal designation. Forced labor due diligence, driven by the Forced Labor Prevention Act and Section 307 import restrictions, requires affirmative supply-chain visibility two tiers deep. Diversion enforcement by the Department of Commerce and Department of Homeland Security increasingly targets the intelligence layer-the transactional evidence that connects a product to a restricted end-user. Your program must evolve or face escalating risk.

Export Controls Now Require Parent-Company and Co-Location Analysis

Most trade compliance teams screen the direct buyer. If the buyer is not on the Entity List or denied-parties lists, the sale appears permissible under the Export Administration Regulations (EAR). This interpretation misses a fundamental shift in how the Department of Commerce enforces export controls on electronics and semiconductors.

A company can avoid listing while remaining subject to export control restrictions if a parent company or ultimate beneficial owner is incorporated in or resides in a country of concern, such as China or Russia. The EAR Part 740 (License Exceptions) and Part 742 (Control of Semiconductor Manufacturing Equipment) establish country-of-origin rules that supersede corporate structure. Similarly, facilities that are co-located with military or government research institutions-even if operationally independent-may fall under licensing requirements for sensitive technologies like advanced semiconductors. Material Change of Circumstances guidance from BIS clarifies that ownership changes, facility acquisitions, or shifts in end-use capability can retroactively trigger export control obligations.

What this means for your program: a subsidiary of a Chinese semiconductor manufacturer, incorporated in Singapore and not listed on the BIS Entity List, may still be subject to licensing requirements under country-of-origin rules if the parent is deemed a "foreign military customer" or "military end-user." Your direct buyer may be clean; the supply chain may not. You need parent-company identification, beneficial-ownership verification, and facility-based intelligence to determine whether licensing applies. This requires moving beyond transactional list screening into structural and relational data-understanding who owns whom, where production occurs, and whether military connections exist. Without this layer, you are screening at the wrong level.

Sub-Tier Supply Chains Harbor Forced Labor and Conflict Minerals Risks

Forced labor risk in electronics manufacturing is concrete. Component manufacturing-semiconductor assembly, printed circuit board production, rare-earth processing-are high-risk sectors. Electronics imports face the highest forced labor risk across G20 nations at $243.6 billion in annual imports.

Forced labor operates in sub-tier suppliers that manufacturers rarely audit directly. The Forced Labor Prevention Act and Section 307 of the Tariff Act establish affirmative due diligence obligations: you cannot rely on a Tier-1 supplier's assurance alone. You must have visibility into Tier-2 and Tier-3 sourcing.

Most programs focus on Tier-1 because direct relationships are manageable. Tier-2 and Tier-3 transparency is fragmented. Suppliers often lack complete visibility into their own sub-tier sourcing for commodity components. This creates a compliance blind spot. Without structured intelligence on sub-tier networks, you depend on self-certification from suppliers who may themselves lack complete knowledge.

Semiconductor Dual-Use Risk and Diversion to Restricted End-Users

Semiconductors present a unique compliance challenge. A single chip design can serve both civilian and military applications. Because the physical product is identical-the difference lies in end-use-traditional product-based screening cannot distinguish civilian from military application.

Diversion-the flow of dual-use products to restricted end-users-is an enforcement priority for both the Department of Commerce and DHS Customs. The approach focuses on the transactional chain, not the product itself. Investigators trace orders and shipments to establish whether a civilian-specification semiconductor ultimately reached a restricted military customer in Russia, China, Iran, or another country of concern. Liability attaches to participation in a supply chain that should have triggered diversion risk signals.

You must understand not just what you are selling but the observable intelligence surrounding who is buying it and for what purpose. If an intermediary buyer with no clear end-customer places unusually large orders, that pattern may signal diversion. If the buyer has facility locations or ownership connections to military research institutions, that relationship may trigger licensing obligations. If transactional history shows rapid re-export to a third party in a restricted country, that pathway indicates diversion risk. These signals are invisible in list-based screening but visible in network and relational data.

Evidence-Based Mapping with Data Lineage as Your Control Framework

Compliance requires moving from list-based screening to evidence-based mapping. Build a control framework that answers four questions: (1) Who are we selling to, including parent companies, beneficial owners, and facility locations? (2) Who are they sourcing from? (3) What is the regulatory obligation? (4) What is the evidence that supports our determination?

The first three require integration of multiple data sources: corporate registration and ownership records, facility geolocation, trade transaction records, and sanctions and export-control lists. The fourth requires data lineage-documenting where information came from, when collected, and how confidence should be assigned. If your screening system flags a buyer based on a single source, your determination is fragile. If the same determination is corroborated by multiple independent sources, your confidence and defensibility are stronger.

This evidence-based approach requires tools beyond traditional list-matching. You need structured access to beneficial-ownership registries, facility-location intelligence, and transactional supply-chain data. You need to visualize networks-understanding how companies connect through ownership and trading patterns. Global trade compliance programs increasingly incorporate this layer because enforcement risk demands it.

Export control, forced labor, and diversion enforcement are accelerating in 2025. Regulators are moving beyond obvious violations to target intelligence gaps-compliance programs that rely solely on list-based screening and miss structural and relational risks embedded in ownership, facilities, and supply-chain networks.

Start by auditing your current approach. Are you screening parent companies? Are you mapping sub-tier suppliers? Are you analyzing transactional patterns for diversion? If not, your compliance framework is incomplete.

Sayari integrates beneficial-ownership intelligence, facility-location data, and transactional supply-chain mapping into a single platform. Customers see a 53% acceleration in screening workflows because the system surfaces non-list-based risk indicators automatically. With access to 8 billion-plus records, the platform enables evidence-based determinations. Learn how Sayari supports your global trade compliance programs-request a demo to see your supply chain mapped.

Please visit sayari.com to learn more.

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