



2026 Export Control Priorities: What Enforcement Tells Us Now

BIS enforcement is escalating and adapting.

Here are the export control compliance priorities that should be shaping programs in 2026 – drawn from enforcement patterns, not rulemaking calendars.

EXPORT CONTROLS

2026 Export Control Priorities: What Enforcement Tells Us Now

By Sayari Analyst Team · Published January 2026

BIS enforcement is escalating and adapting. Here are the export control compliance priorities that should be shaping programs in 2026 – drawn from enforcement patterns, not rulemaking calendars.

Export control compliance has been transformed from list-checking to ownership-and-end-use investigation. Ten years ago, export control was back-office work: screen against the Entity List, confirm no Denied Persons List match, classify as EAR99, ship.

That model is no longer sufficient. Since 2022, the Bureau of Industry and Security (BIS) and Department of Justice have pursued a different enforcement approach entirely. The focus has shifted from whether a company exported to a listed party to whether it understood where products were ultimately going, who actually owned the buyer, and whether the transaction fit a pattern of evasion. BIS has backed this shift with the most significant expansion of US export controls since the Cold War.

Companies that operated compliant export programs in 2020 are facing criminal and civil liability in 2026 because the compliance standard itself has changed. The gap between list-checking and current enforcement expectations is where the enforcement risk lives.

Priority 1: China semiconductor and advanced technology controls

The October 2022 BIS semiconductor rules marked the largest single expansion of US export controls in four decades. The rules restricted exports of advanced semiconductor equipment and design tools to China, including intermediate nodes previously available. In October 2023, BIS closed what it characterized as "loopholes," tightening the definition of controlled items and restricting additional advanced semiconductor manufacturing equipment.

The Huawei Mate 60 Pro, appearing in August 2023, demonstrated that some advanced semiconductor capacity was reaching China through unanticipated routes. The phone incorporated a 5-nanometer processor sourced through Samsung and TSMC suppliers, suggesting transshipment through third-country intermediaries or exploitation of control gaps.

Current enforcement shows BIS prosecuting companies that exported semiconductor manufacturing equipment and design tools to China, directly or through subsidiaries. The enforcement net extends beyond the Commerce Control List-BIS has pursued cases involving items initially classified as EAR99 when export patterns and end-use showed intent to support China's semiconductor capacity.

BIS has coordinated with Japan and the Netherlands to restrict exports of chipmaking equipment-specifically advanced lithography systems from ASML. This "trilateral" coordination reflects the recognition that unilateral US controls can be circumvented if other semiconductor equipment exporters don't align.

The 2026 priority is clear: semiconductor equipment, components, and design tools destined for China face the highest enforcement attention. Companies in this supply chain need to understand their beneficial end-users, not just immediate customers.

Priority 2: Russia sanctions evasion through dual-use goods

Large civil penalties demonstrate escalating enforcement. Applied Materials paid \$252 million in February 2026-the second-largest BIS penalty in history, with the largest being Seagate's \$300 million settlement in 2023. These cases involve dual-use items: microelectronics, aviation components, semiconductors-goods with legitimate civilian applications that also enable military capability. Enforcement data shows items being transshipped through intermediaries in Turkey, the UAE, Armenia, and Kazakhstan, with buyer patterns showing hallmarks of coordinated evasion.

BIS publishes "red flag guidance" for Russia evasion transactions. Indicators include new customers with no prior trading history, payment in full upfront, unusual shipping routes, reluctance to discuss end-use, and purchases of complementary items (microcontrollers plus power supplies plus thermal management components). Multiple flags across several transactions show intent.

DOJ's National Security Division has increased criminal export control prosecutions since 2022, targeting individuals and companies rather than isolated transactions. Criminal cases

charge conspiracy: the company and individuals knew exports were destined for Russia military end-use, coordinated transshipment, and concealed the transaction.

Third-country transshipment is not a defense. BIS and DOJ can pursue US companies for exports to Turkey, UAE, Armenia, or Kazakhstan if evidence shows knowledge that goods would be transshipped to Russia.

The 2026 priority is Russia evasion prevention, requiring monitoring of both direct customer orders and trade patterns indicating transshipment networks.

Priority 3: End-user screening has moved beyond the Entity List

The BIS Entity List, OFAC's Specially Designated Nationals list, and State Department ITAR restricted parties comprise approximately 40,000+ restricted parties globally. But enforcement data shows a different pattern: companies are being prosecuted for exports to entities that never appeared on a list.

The answer is beneficial ownership. A restricted party can operate through corporate proxies, subsidiaries, or intermediaries that don't themselves appear on any list. If a listed Chinese technology company acquires a stake in a Singapore semiconductor distributor, the Singapore entity isn't automatically listed. But under current BIS enforcement expectations, a US exporter selling to the Singapore entity can be held liable if there is evidence of knowledge of the beneficial ownership structure.

A company can screen against the Entity List and pass. But if it didn't perform due diligence on beneficial ownership-checking corporate registries, conducting web search, requesting customer information about parent companies-it hasn't met the current enforcement standard.

BIS guidance on "know your customer" practices has become enforcement guidance. The standard is: what would a reasonable export compliance officer have discovered through diligent investigation? If the answer is "the beneficial owner was listed" and the company didn't discover it, the company is liable.

Companies selling components to distributors in the UAE or Turkey face an implicit due diligence burden: understand whether those distributors are connected to restricted end-users. Enforcement cases show criminal liability when companies exported to distributors without performing basic corporate research.

The 2026 priority is moving from list-checking to owner-and-end-user verification.

What a 2026-ready export compliance program actually requires

Export compliance programs relying on automated list-checking and standard customer questionnaires are no longer sufficient. BIS and DOJ are investigating entity resolution, trade flow analysis, and continuous monitoring.

First, entity resolution-connecting export counterparties to their beneficial owners. This requires access to corporate registry data across jurisdictions, cross-border investment data, and trade data revealing actual relationships.

Second, trade flow analysis-identifying patterns suggesting transshipment. If a UAE company orders microelectronics in volumes far exceeding what a legitimate distributor would need, that's a red flag. If product specifications are incompatible with known civilian end-uses, that's a red flag.

Third, continuous monitoring. A counterparty can be compliant at time of sale and restricted months later due to sanctions or entity list updates.

Companies that exported in 2020 under a compliant program are facing criminal referral in 2026 because the enforcement standard changed. Export compliance now requires investigation, not just screening.

Sayari's Global Trade Compliance software integrates entity data from corporate registries, beneficial ownership records, trade data, and sanctions lists to address this enforcement shift. The platform combines 10.6 billion+ primary-source records, 4 billion trade transactions, and coverage across 250+ jurisdictions - enabling export compliance teams to perform entity resolution, beneficial ownership screening, and trade pattern analysis at the scale modern supply chains require.

The 2026 export control environment will reward programs built on investigation, not just list-checking. Request a demo to see how modern compliance programs are adapting.

Please visit sayari.com to learn more.

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