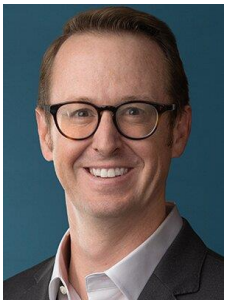
LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3rd-Party Audit Tactics To Improve Export Control Compliance

By **Michael Huneke, John Rademacher and Abby Williams** (July 7, 2025, 5:16 PM EDT)


Michael Huneke


John Rademacher


Abby Williams

Export controls are a critical tool used by the U.S. to constrain foreign adversaries' access to sensitive U.S. technologies. Despite increasingly complex and robust export control requirements, U.S. technologies reportedly continue to be smuggled to China in violation of the U.S. export controls' catch-all provisions.

This follows prior reports, based on battlefield recoveries by Ukraine and nongovernmental organizations, of smuggled U.S. technologies fueling Russia's ongoing war in Ukraine, either by diversion to Russia or diversion through embargoed countries, such as Iran and North Korea, that are supplying Russia with weapons systems.

Both cases threaten U.S. economic and national security.

Foreign adversaries have reportedly evaded export controls, potentially in large numbers, presumably by successfully concealing the actual intended end user, end use or end destination of exports restricted under the U.S. Department of Commerce's Export Administration Regulations, or EAR.

They have done so by exploiting control weaknesses of second- or even lower-tier distributors, dealers and resellers.[1] In April, a subcommittee of the U.S. House of Representatives concluded that DeepSeek, for example, was built using stolen U.S. technology that is prohibited from sale to China without an export license.[2]

Despite these challenges and geopolitical realities, companies can more effectively assess third parties' export control compliance to detect circumvention of export controls.

The Export Control Regulatory Landscape

Since taking office in January, the administration has pursued trade and economic policies that prioritize the U.S. economy and its national security interests. On President Donald Trump's first day in office, the White House issued the America First Trade Policy directive, instructing the secretaries of the U.S. Department of State and the U.S. Department of Commerce to recommend measures to eliminate loopholes in existing export controls and strengthen export control enforcement policies and practices.[3]

The America First Trade Policy followed on the heels of findings by the majority staff of the U.S. Senate's Permanent Subcommittee on Investigations. Those findings concerned how the Commerce Department's Bureau of Industry and Security, or BIS, could significantly increase export controls compliance and enforcement. This could be achieved by imposing higher fines on companies who violate export controls and leveraging the full definition of "knowledge" under the EAR.

The EAR's definition of knowledge includes both "reason to know" and "an awareness of a high probability," both short of "actual knowledge," when companies fail to sufficiently investigate red flags indicating a potential diversion of restricted products.[4] The subcommittee had further recommended increases in funding for BIS to increase staff and replace outdated systems.

In its fiscal year 2026 budget proposal to Congress, the administration proposed more than a 50% increase in BIS funding to protect U.S. technological competitiveness and counterthreats from China.[5]

More broadly, on May 12, the U.S. Department of Justice announced that its Criminal Division is prioritizing the investigation and prosecution of corporate crimes that pose the greatest risks to U.S. interests. In particular, this involves focusing its resources on threats to the U.S. economy and national security, which closely aligns with export controls.[6]

Circumvention of Export Controls

Foreign adversaries often exploit or allow others to exploit weaknesses in companies' internal controls designed to prevent exports destined for inappropriate end uses, end users or end destinations. This frequently involves the diversion of products through third-party distributors, dealers and resellers.

The BIS has published red-flag indicators that may signal a planned unlawful diversion, such as:

- The customer has a limited business background;
- "The customer … is reluctant to offer information about the end-use of a product";
- "The product's capabilities do not fit the customer's line of business";
- "The customer is unfamiliar with the product's performance characteristics," or declines installation, training or maintenance services; and
- "The shipping route is abnormal for the product and destination," or a freight forwarder or logistics company (or, similarly, a free zone or general trading company) is listed as the product's destination.[7]

Companies cannot be self-blinding to these red flags. When they have knowledge of red flags, including an awareness of a high probability that a violation has occurred, they must investigate the circumstances to determine the end use, end user or ultimate country of destination of exports, both under a fair reading of the high-probability standard and in accordance with the BIS' "'Know Your Customer' Guidance and Red Flags."[8]

Anticipating that the administration is only going to increase, rather than decrease, its expectations for preventing diversion to adversaries, companies can take steps now to enhance their ability to assess the compliance of their distributors, dealers and resellers with U.S. export controls.

Enhancing Third-Party Audits

Quality Over Quantity Using a Risk-Based Approach

The subcommittee's inquiry found that some of the largest semiconductor manufacturers do not audit the export controls for all their distributors on a yearly basis, while some manufacturers do not conduct routine audits of their distributors for export controls at all.

This poses a significant risk for companies that sell technologies with a high likelihood of diversion. This is particularly true if the company ignores red flags or disregards information that could indicate a third party may have diverted goods, or if its employees willfully avoid facts suggesting potential misuse.

Though companies may not have sufficient resources to audit — in the traditional sense of internal audit and compliance protocols — the export controls of all their distributors on a yearly basis, companies should consider a risk-based approach to identifying third parties that pose the highest risk of noncompliance with export controls.

This dovetails with the layered definition of knowledge under the EAR and, importantly, allows the company to focus deeper audits on its highest-risk third parties, as opposed to conducting more limited desktop reviews of a broader number of third parties.

If misconduct comes to light after the fact, companies that conducted a thorough, risk-based diligence process that can best defend how and where they identified their highest risks will be better off than companies that took a one-size-fits-all approach or looked at everything with the same level of probity.

Although the specific risk factors that would best inform a risk-based approach to selecting third parties will vary by industry, geography and company, in general, companies could start by considering the following factors when assessing relative compliance and enforcement risks under U.S. export controls:

- Abnormal orders — orders from new customers or sudden changes in the frequency, volume or value of orders from existing customers;

- Transshipment red flags — shipments to or through countries identified at higher risk of transshipment, including the United Arab Emirates, Turkey, Malaysia and Singapore, among others;

- Abnormal shipping patterns — shipments directly to freight forwarders or other entities that do not appear to be the customer;

- Geopolitical events — significant changes to purchasers or quantities around key geopolitical events, e.g., announcements of new or contemplated controls;

- Abnormal payments — customer payments originating from multiple bank accounts, accounts in restricted or transshipment countries, or cash payments despite financing terms;

- Product sensitivities — products with an increased risk for diversion or misuse; and

- Internal observations — customers identified by sales and accounting teams that may be aware of red-flag indicators in the normal course of business.

These risk factors and others may be incorporated into a risk-scoring model to identify the company's highest risk third parties to audit.

Steps Beyond Desktop Reviews

Frequently, companies conduct third-party audits that are limited to desktop reviews or rely upon self-certified third-party compliance questionnaires. These audits often involve only cursory reviews of trade compliance policies, limited interviews and minimal sample testing to assess whether end-user certifications and other trade compliance forms have been retained.

Companies may also include limited procedures for export controls in the context of broader third-party audits focused on compliance with commercial terms or anti-bribery and corruption. These types of audits, however, may miss key export control risks due to the limited nature of the procedures.

For the highest-risk third parties, companies should consider probing further by going beyond a desktop review of export control documentation. This may include several approaches.

One option is targeted interviews of a broader set of employees.

Companies can use interviews with sales personnel to evaluate their understanding of the customer's end use of the goods, how the goods will be used within the customer's line of business, whether the customer demonstrates familiarity with the product's performance characteristics and whether the customer needs installation, training or maintenance services, among other indicators.

Further, interviews with accounting personnel can help companies understand and flag unusual billing practices, the use of third-party payment methods — e.g., payment from someone other than the buyer listed in the sales contract — or unusual financing terms that could signal an increased risk of diversion.

And interviews with logistics personnel can help companies understand and flag high-risk shipping practices, use of freight forwarders and unusual shipping terms — e.g., international commercial terms, also called Incoterms.

A second option is to compare sales data against compliance data to identify gaps that may suggest false certifications, misrepresentations during onboarding or concealment of risk factors.

This may include reconciliation of sales-related data such as invoiced amounts, location, customers, products with compliance-reported data, due-diligence questionnaires, third-party declarations, representations in contracts and certifications.

A third option is to conduct a targeted email review prior to the third-party audit to understand the commercial substance of the transaction and end use of the restricted product, as well as to identify red flags that may suggest an awareness of diversion risks, attempts to bypass licensing requirements or inconsistent statements about end use.

Verification is a fourth option. Depending on the risk level of the transaction or product, companies should consider actively verifying customer legitimacy. This may include requesting photos of the facility

where the product will be used, confirming contact details through direct email or phone outreach, or conducting a virtual or in-person site visit.

Increased Use of Forensic Analysis

Foreign adversaries are adept at circumventing export controls by concealing the true beneficial owners of businesses. Often times, red flags may be present that demonstrate this risk, including businesses with limited online presence, businesses located at or near the address of an entity on the Commerce Department's entity list, or newly formed businesses.

Companies may be better equipped to identify red flags involving the highest-risk third parties by conducting searches using open-source research tools, semi-publicly available resources and local intelligence. These tools can help uncover the ownership structures, pertinent connections, backgrounds and reputations of third parties.

Key Takeaways and Path Forward

Foreign adversaries have successfully evaded export controls by concealing the actual intended end user, end use or end destination of exports restricted under the EAR, oftentimes exploiting control weaknesses of distributors, dealers and resellers.

Senior figures in the administration, most notably through the State and Commerce departments, are intent on eliminating loopholes in export controls and enhancing export control enforcement.

This may include imposing higher fines on companies that violate export controls and charging companies with knowing violations when they fail to sufficiently investigate red flags of potential diversion.

Additionally, the DOJ is prioritizing investigations of corporate crime that will have the greatest impact in promoting U.S. interests and protecting U.S. national security.

To identify sophisticated and high-risk diversion schemes, companies should consider first which criteria to use to identify their highest-risk relationships and, for those relationships, go beyond the typical know-your-customer screening and reliance on self-certifications as to end use or end user.

By going beyond a cursory desktop audit and supplementing typical audit procedures with targeted interviews of back-office functions, email review and verification, companies can better position themselves to defend the calibration of their risk assessment.

Increasing the use of forensic analyses will also help companies protect themselves when, invariably, something is missed.

Michael H. Huneke is a partner and a co-chair of the sanctions, export controls and anti-money laundering practice group at Hughes Hubbard & Reed LLP.

John Rademacher is a managing director at Secretariat Advisors LLC.

Abby Williams is a director of global investigations and disputes at Secretariat Advisors.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] The U.S. Technology Fueling Russia's War in Ukraine: Examining Semiconductor Manufacturers' Compliance with Export Controls.

[2] DeepSeek Unmasked: Exposing the CCP's Latest Tool For Spying, Stealing, and Subverting U.S. Export Control Restrictions.

[3] America First Trade Policy – The White House, January 20, 2025.

[4] The U.S. Technology Fueling Russia's War in Ukraine: Examining BISs Enforcement of Semiconductor Export Controls, dated December 18, 2024.

[5] Fiscal Year 2026 Discretionary Budget Request.

[6] Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime, Department of Justice, May 12, 2025.

[7] Supplement No. 3 to Part 732—BIS's "Know Your Customer" Guidance and Red Flags.

[8] Id.