Export controls on advanced tech: Managing supply chain risk

Forensics Today

PwC perspectives on the newest risks drawing investigator scrutiny

pwc

- Export controls have expanded significantly to protect US national security and technology leadership in semiconductors and emerging technologies like artificial intelligence. It's likely they'll expand further to cover more innovations and entities.
- These controls have disrupted global supply chains, affecting how companies source parts, manufacture components and navigate international markets.
- To succeed, organizations should fully understand these restrictions, maintain compliance and adapt their overall strategy, sourcing and products accordingly.

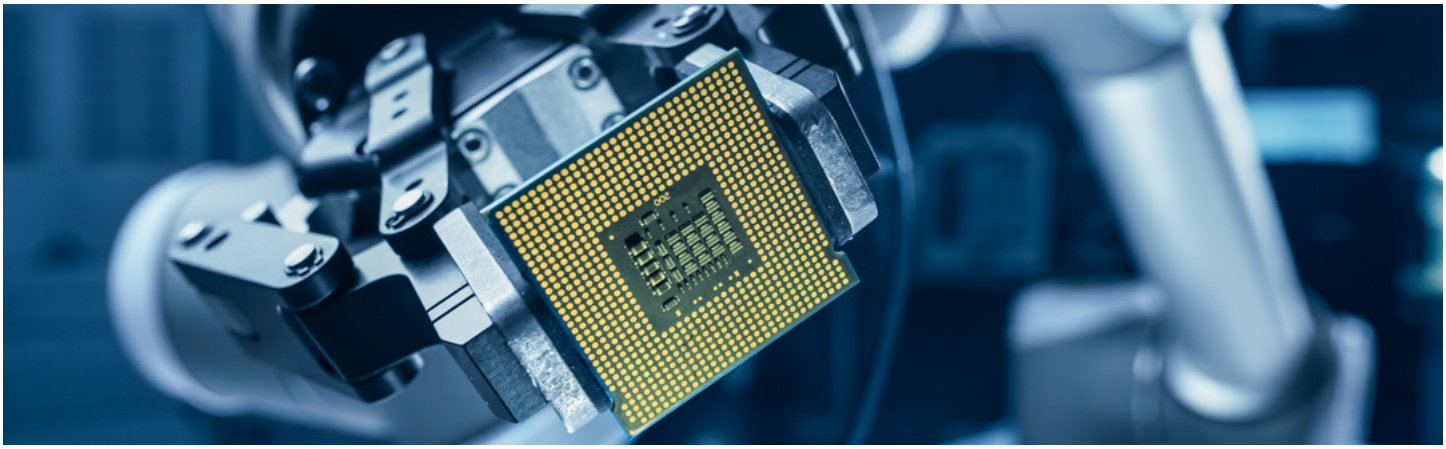
Export controls continue to be a key instrument of the US government's efforts to develop and preserve a technological competitive advantage under an expanding national security umbrella. These trade restrictions on advanced technologies have led companies to reassess their end-to-end product life cycles, including a reevaluation of strategic sourcing efforts and procurement decisions, as well as exports of US-origin parts and components for manufacturing and final assembly abroad.

Take, for example, companies that source items from China, such as semiconductors and advanced tech components. Many are now considering a potential pivot to secure alternate suppliers and are actively reducing reliance on longtime partners and regions. This has resulted in manufacturing disruptions, product delays and the need to move production to other countries.

Some companies are also considering their options for fulfilling orders abroad in alignment with shifting regulatory requirements and the evolving use of tariffs as a foreign policy tool. This growing complexity and these recent shifts are impacting organizations with extensive, global value chains, pushing them to adapt business models to mitigate risk and maintain operational efficiency.

Capitalizing on this trend, nations like Mexico, Vietnam and others in Southeast Asia, are emerging as key players in the semiconductor and technology supply chain, stepping in to fill the gap created by tension surrounding US-China trade. These countries offer lower-cost production alternatives while avoiding the regulatory pitfalls that come with dealing directly with China. The United States, too, has authorized funding to incentivize domestic research and manufacturing of semiconductors, via the CHIPS Act.

Affected companies should reevaluate their sourcing approach and invest in infrastructure to navigate these export controls and assess opportunities to onshore efforts. This includes integrating compliance into business strategy, operations and product design.



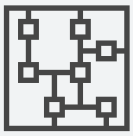
Chip and tech controls proliferate, accelerate

In this new era of strategic competition, US export controls have increasingly targeted China's access to American-made semiconductors — and, by extension, any products that contain these semiconductors such as servers and laptops. Coupled with the CHIPS Act, these measures are designed to protect US national security and bolster US tech leadership amid rising competition from China. Activity has accelerated across recent administrations, and we expect this to continue under the Trump White House with further measures limiting China's access to US innovations and an increased focus on strengthening the domestic tech sector.

Key rules and guidance have been issued in recent years by executive agencies and committees tasked with protecting critical US technology.

October 7th rule

In 2022, the Commerce Department's Bureau of Industry and Security (BIS) expanded existing controls, specifically targeting China's ability to acquire integrated circuits, semiconductors critical to advanced computing, AI and other emerging technologies. The rule effectively banned the export of advanced chips, chip manufacturing tools and certain tech components to China, even indirectly through third-party countries or entities. It also imposed licensing requirements on US companies selling these technologies to certain Chinese entities, aiming to curtail China's development of military-grade AI systems and other national security-sensitive technologies.



October 17th rule

In 2023, BIS introduced new parameters, such as performance density measures for integrated circuits, designed to close loopholes that could allow Chinese companies to circumvent earlier restrictions. It also extended licensing requirements to other countries, including Vietnam and Egypt, to prevent these nations from acting as intermediaries for rerouting restricted technologies to China.

"Reset, prevent, build" strategy

In December 2023, the House select committee on competition with China outlined a strategy for a complete overhaul of US-China trade relations, focusing on restricting US investments in Chinese companies developing critical technologies like AI and semiconductors, especially those linked to China's military.

Advanced tech export control rule

In September 2024, BIS issued new export controls on semiconductors, quantum technologies and additive manufacturing, aligned with international partners. The rule added new export control classification numbers (ECCNs) and licensing requirements, reflecting a coordinated global effort to protect national security and foreign policy interests.

Outbound investment security program

In October 2024, the Treasury Department issued a rule implementing a program to restrict outbound investments by US persons in certain entities controlled by foreign rivals, as required by an August 2023 executive order.

Limits on tech for military use

In December 2024, BIS restricted China's ability to source and build semiconductors, AI and advanced computing technologies for military applications. These rules include restrictions on chip manufacturing equipment, software tools for producing chips and high-bandwidth memory, along with additions to the Entity List, improvements to previous controls, and guidance to address compliance and diversion concerns.

Bulk sensitive data transfer limits

In December 2024, the Treasury Department issued a rule imposing stringent limits and oversight mechanisms on the collection, processing and cross-border transfer of bulk sensitive data by foreign rivals, as required by a February 2024 executive order. The data in question includes sensitive personal information about US individuals — health, financial, geolocation, biometric and genomic data — as well as government-related data.

"America-first" trade policy

In January 2025, President Trump ordered the State and Commerce Departments to review the US export control system, including enforcement policies and mechanisms, and recommend improvements to strengthen the nation's technology edge. In particular, the order seeks "to identify and eliminate loopholes in existing export controls — especially those that enable the transfer of strategic goods, software, services, and technology to … strategic rivals and their proxies."

These measures coincide with similar efforts abroad, as the United States works closely with allies like the European Union, Canada and Japan to create aligned export control regimes. The result is an increasingly elaborate mosaic of global restrictions. According to PwC's Global Economic Crime Survey 2024, 59% of executives surveyed agree that export controls have grown more complex and more than half (51%) believe export controls are being enforced more robustly than two years ago.

A path forward: Applying the known, anticipating the unknown

Recent and anticipated regulatory actions by the Trump administration coupled with an increasingly tense geopolitical environment clearly affect companies that trade with China or work with controlled technologies. To remain compliant and competitive, you'll need a clear plan to navigate these requirements and safeguard your operations.

As a critical initial step, many companies are engaged in scenario planning to assess whether and how their organization and value chains may be impacted under the evolving regulatory regime. They're evaluating the extent and potential severity of impact to their business models and operations, providing a foundation to reassess strategies. They're also reflecting on sourcing, development, manufacturing, sales and people processes and considering steps that allow for compliance coupled with agility to handle other potential restrictions. Finally, they're implementing necessary adjustments and appropriate change management measures to mitigate the risk of future noncompliance while continuously monitoring and integrating new regulations into their compliance programs.

Consider this case study…

Company A is a US-based multinational tech company with a global supply and distribution chain handling integrated circuits that are designed domestically with components procured from China, manufactured in Vietnam and supported by US persons abroad.

- **Risk assessment:** As these geopolitical dynamics unfold, Company A conducts a risk assessment and identifies new regulations that may impact its supply chain and ability to use US resources abroad, particularly in the Asia-Pacific region.
- **Strategy development:** To remain nimble, Company A considers adapting its sourcing strategies to navigate the shifting regulatory landscape — especially the evolving use of US tariff policy — and develops a proposed shorter- and longer-term strategy for its people and manufacturing operations.
- **Program enhancement:** Company A then strengthens its existing compliance infrastructure, incorporating enhanced oversight of the sourcing, movement and licensing of critical emerging tech components. It takes concrete steps to implement clear protocols such as drafting new policies, procedures and technology control plans (TCPs) to identify and safeguard export-controlled items like semiconductors and advanced technologies. It also implements a new restricted-party screening tool and undertakes risk assessments of third-party partners to support compliance across the value chain.
- **Organizational readiness:** Company A implements change management protocols related to program enhancement and new strategic direction, including determining affected stakeholders, developing a training plan and delivering communication to increase awareness across impacted relevant parties and business units.
- **Monitoring:** To stay ahead of regulatory changes, Company A develops robust oversight mechanisms that actively monitor and track regulatory changes, supply chain vulnerabilities and new licensing requirements. It also establishes relationships with specialists who can provide guidance on the latest regulatory updates, helping the company to stay compliant while maintaining operational efficiency.

Bottom line

It's imperative to review your sourcing strategies, product life cycles and compliance infrastructure in light of existing and potential export controls on advanced tech. The same goes for your shipments of restricted components for manufacturing and assembly abroad. Success will require conducting scenario-planning and adjusting your strategy, products and compliance programs to meet these restrictions, while also bolstering your organization's overall agility to adapt to ongoing regulatory and geopolitical uncertainty.

Contact us

Ryan Murphy
Partner, Global Investigations & Forensics Leader, PwC US
ryan.d.murphy@pwc.com
LinkedIn

Amanda Cox
Principal, Financial Crimes Practice Leader, PwC US
amanda.cox@pwc.com
LinkedIn

George Prokop
Principal, Cyber, Risk & Regulatory, PwC US
george.w.prokop@pwc.com
LinkedIn

Eric Lorber
Principal, Cyber, Risk & Regulatory, PwC US
eric.lorber@pwc.com
LinkedIn

pwc

www.pwc.com