Law Practice Today

Why All Lawyers Need to Understand the U.S. Export Control System

David Levine

Aug 15, 2024

Summary

- Export controls are regulatory measures that specify which goods and technologies require a license before they can be exported to certain countries or end users.
- The U.S. has expanded export controls to regulate outbound investments in sensitive technologies and services, including cybersecurity and artificial intelligence, with a focus on national security concerns.
- Export control specialists are crucial in both overseeing exports and reviewing foreign acquisitions of U.S. companies, especially as CFIUS increasingly relies on export control regulations to assess national security risks.

I was at the bike rack outside my son's elementary school this spring, waiting for a parent-teacher conference, when I got a call from a client: Would there be any concern with shipping wedding dresses wholesale to Russia? Ten years ago, this would have been a straightforward question to answer: Of course not; there are no (as far as I know) military-grade wedding dresses, and, regardless of how intricate, wedding dresses cannot be incorporated into advanced weapons systems. Since the invasion of Ukraine, however, the U.S. and its allies have put in place increasingly restrictive controls on the products allowed to be sent to Russia that have captured goods beyond traditionally military-linked items. So the answer in the case of the wedding dresses was, as it turns out, "it depends" (on the quantity, material, and price of the dresses) because certain garments are considered "luxury goods" that are now covered by the new controls.

Export controls have become an increasingly important tool in the United States' policy toolkit over the past decade. Both the Trump and Biden administrations have used the country's ability to control the flow of goods and technology beyond our border to answer the varying threats they faced around the globe, most prominently from China and Russia. Export controls' increasing prominence as a policy tool means that lawyers in a variety of practice areas should take the time now to become familiar with the structure and substance of the U.S. export control system — or have someone on speed dial who is.

For the uninitiated, "export controls" are precisely what they sound like — calibrated controls, implemented through regulation (most notably the International Traffic in Arms Regulations, or ITAR, and the Export Administration Regulations. or EAR), that identify specific goods and technology that may not be exported to certain countries or end users without a license. Export control specialists consult with clients seeking to sell their wares in new markets. They also conduct due diligence for transactions involving companies that make and export defense-related or dual-use goods, ensuring compliance procedures are followed and past violations are ferreted out.

In the modern legal and national security environment, however, knowledge of export controls is becoming more important for more attorneys. Not only are a greater number of goods coming within the purview of export control enforcement agencies, but the increased prominence of the Committee for Foreign Investment in the United States (CFIUS) in reviewing mergers, acquisitions, or investments involving foreign owners of U.S. companies means that export control lawyers have an even larger role to play in deal work. Even more importantly for most lawyers, though, the U.S. government is continuing to either impose export controls or use the export control system in novel ways.

Formerly a niche field, the United States' increasing reliance on export controls to set the terms of its economic engagement with the rest of the world means that attorneys across the spectrum of practice areas will need basic literacy in the area.

Increased Reliance on Export Controls in the International Arena

Export controls had been regarded as a relative legal backwater during much of the postwar period. Controls were generally applied to a relatively narrow cross-section of goods — either purely military goods or civilian goods that were likely to be used for military purposes (so-called "dual use" goods). Export controls were viewed as technical and intended to keep strategically important or particularly advanced technology out of the hands of specific rogue or unfriendly regimes.

Increasingly, however, the United States has turned to export controls as a tool for containing geopolitical rivals and countering crises. Under the Trump administration, with its desire to fulfill campaign promises for a more aggressive approach to China, the United States used export controls as another economic weapon in the promised trade war. The Trump Commerce Department pioneered using export controls to starve Chinese technology companies, specifically Huawei, of semiconductors and related machinery used to make their most advanced products. Many observers expected the Biden administration to reverse course and effectively return export controls to the technocratic province they had been previously. Those expectations, however, were confounded by the one-two punch of a bipartisan appetite for continuing pressure on China and the Russian invasion of Ukraine. Instead of repealing Trump's actions, the Biden administration put them on firmer legal footing and then used them as a blueprint for its own efforts to undermine Russia's war machine and ratchet up pressure on China. The list of items prohibited for export to Russia (or its Belarusian client) has grown ever longer since February 2022, and restrictions on the export of high-end computer chips (or the machinery to manufacture them) to China have made front-page news.

As a result, the number of U.S. businesses with potentially export-controlled products has skyrocketed. The current export controls on Russia run the gamut from advanced petroleum extraction machinery components to tobacco refuse (another product identified as a so-called "luxury good," presumably due to its use in cigarettes) and everything in between. Virtually any good used in semiconductor manufacturing and destined for China, down to the smallest purpose-built gasket, could be subject to stringent licensing provisions if it is intended for use in a factory making certain advanced semiconductors. Moreover, even if a U.S. business's immediate customer is not in Russia or China, it might still be liable for export control violations if it should have known its products were destined for such restricted end users. Accordingly, lawyers with clients who make any sales overseas should have their eye on the recent, and almost certainly ongoing, expansion of export controls.

Export Controls Are Critical to Mergers and Acquisitions with an International Nexus

Beyond their role in counseling clients who send goods and technology overseas, export control specialists have always had a role to play in the buying and selling of companies. Traditional diligence of companies with overseas touchpoints has long necessitated a review of which products are being sent to which foreign countries, and who is using them when they get there. The importance of that role has escalated as the U.S. export control agencies have increasingly taken an interest in software and technology over the last three decades. But fundamentally, the role of an export control lawyer in the diligence process has remained stable: confirm that a company is not sending controlled items to locations or end users that are prohibited from receiving them.

Increasingly, however, export control specialists are called on to play a role in reviewing acquisitions of U.S. companies by foreign investors. Recent updates to CFIUS's regulations have built on and used export control regulations as a basis for CFIUS's control, which means that evaluating regulatory risks for deals involving foreign parties will necessarily involve an export control analysis. CFIUS has jurisdiction to review acquisitions or investments by foreign parties that might implicate U.S. national security concerns. As a proxy for identifying transactions where such concerns might be present, CFIUS "piggybacks" on the U.S. export control system. Effectively, CFIUS does not want foreign entities using mergers and acquisitions as a backdoor around export control restrictions. Accordingly, in cases where a license would be required to export technology to the acquirer's home country, a CFIUS filing may be mandatory and the parties may need to receive approval before the transaction can be consummated. This requirement has been particularly salient for companies with in-house software that incorporates encryption functionality; such products are generally eligible for a license exception with minimal effort, though if the software is offered as a SaaS product or used internally, the company would have had no reason to apply for an exemption prior to engagement with the CFIUS process. Accordingly, deal lawyers need to involve export control specialists from an early stage to identify and classify potential export-controlled items and technology, or risk potentially catastrophic consequences (up to and including mandated divestment).

Using the Export Control System in Novel Areas

The U.S. has also begun using the export control system to address new national security concerns. In 2023, the U.S. Department of Treasury released its long-awaited plans to begin regulating certain outbound investments; those plans were followed up with a more concrete proposed rulemaking this summer. Known colloquially as "outbound CFIUS," the proposed regulations identified certain overseas investment categories that could have adverse impacts on U.S. national security, such as investments in artificial intelligence or supercomputing resources in China. As the traditional CFIUS regulations have done, in order to identify specific investments that might reasonably cause national security concerns, Treasury made use of the classifications already in place within the Commerce Control List (the primary list of dual-use items subject to export controls), specifically with respect to semiconductors. Though the proposed rules remain subject to public comment for now, the proposed scheme means that for certain categories of foreign investments, U.S. individuals and entities may need to conduct an export control classification of the products of the investment target, regardless of the fact that the goods themselves may never enter (much less be exported from) the U.S.

Similarly, the office that traditionally enforces most U.S. export controls is also expanding its regulatory purview. The Department of Commerce's Bureau of Industry and Security (BIS) has traditionally been charged with licensing and enforcing the dual-use export control system (that is, export controls for items that are not strictly military-related), as well as anti-boycott laws. Recently, however, it has added the Office of Information and Communications Technology and Services (ICTS), whose remit stretches beyond businesses and persons who might typically think of themselves as exporters or even engaged in international commerce.

ICTS's most recent regulatory action puts the new office's reach in stark relief. On June 20, 2024, ICTS issued a "final decision" determining that cybersecurity and anti-virus software sold by the Russian-based company Kaspersky posed an "undue and unacceptable risk to U.S. national security." As a practical matter, this final decision bans Kaspersky from selling its popular anti-virus software or providing services to all customers in the United States and set off a scramble among U.S. chief information security officers to transition to a nonbanned alternative. This was the first time ICTS used authority granted to it under an executive order meant to help secure U.S. supply chains, and the office targeted software used widely by both individuals and businesses. The Kaspersky final decision may provide a blueprint for the office's future actions and illustrates the need for businesses with connections to vet their overseas touchpoints — even those as seemingly mundane as anti-virus software — with an eye toward potential national security risks. As the expansion of traditional export controls over the past five years demonstrates, companies with connections to Russia and China should be particularly vigilant for future ICTS actions.

Even clients who perceive themselves to be running a purely domestic business may have a need to become familiar with ICTS. In January 2024, ICTS issued a notice of proposed rulemaking that put providers of what the notice called "Infrastructure as a Service (IaaS)" that they may have to begin conducting enhanced diligence into certain customers. IaaS products include cloud services and other businesses that provide computing resources to customers. There has been a persistent concern that foreign persons — and particularly Chinese entities — could attempt to circumvent the recent semiconductor and advanced computing-related export controls by simply paying to access the same resources provided by U.S. suppliers. So, for instance, instead of acquiring an advanced U.S.-origin computer chip, a company could pay to access the capabilities of the chip via the cloud and a domestic U.S. company. Moreover, news reports from this spring indicate that ICTS is considering similar measures with respect to providers of artificial intelligence models. These initial forays into information technology service regulation are undoubtedly focused on a specialized high end; however, as with traditional export controls, which have expanded from rocket motors to wedding dresses, it is not a stretch to envision ICTS controls expanding to more run-of-the-mill services in the future. While ICTS's plans for regulating such service providers are in a preliminary stage, it is quite likely that the final implementation will build on the export control infrastructure already in place within BIS more broadly.

In recent years, export controls have expanded beyond their previously limited reach and begun to impact an ever-increasing slice of American commerce. The U.S. government has increased the sheer number of products subject to some form of control but has also begun using the export control infrastructure to combat a growing list of national security threats. And, though primarily the realm of regulatory agencies, because of the significant deference given in matters of national security, export control regulations are unlikely to be impacted by the fall of Chevron. Accordingly, attorneys across a growing list of practice areas and specialties will need to have at least a passing familiarity with the structures and mechanisms of export controls in order to effectively serve their clients.

This article was originally published by the Law Practice Division in Law Practice Today on August 15th, 2024.

Authors

David Levine

Willkie Farr & Gallagher LLP

David Levine is an attorney in the Global Trade and Investment practice group at Willkie Farr & Gallagher LLP, where his practice focuses on export controls, sanctions, and other national security-related matters. ...