7 Enforcement Predictions For US Export Controls, Sanctions

By **Jonathan Poling, Ryan Fayhee and Tyler Grove** (December 12, 2023)

Jonathan Poling

Ryan Fayhee

Tyler Grove

Within the trade bar there is cautiousness, curiosity and skepticism at the numerous pronouncements signaling greater enforcement of export controls and sanctions by the Bureau of Industry and Security, the Office of Foreign Assets Control and the U.S. Department of Justice.

The U.S. Department of State's Directorate of Defense Trade Controls has been noticeably absent from these enforcement initiatives, though the underlying reason is not clear.

Across the administration, speeches, press releases, announcements and industry outreach efforts, consistently messaging a new era of increased enforcement, are plentiful. The deputy attorney general of the DOJ recently proclaimed that sanctions are the new Foreign Corrupt Practices Act. The number of prosecutors in the National Security Division of the DOJ is expected to double.

A great number of task forces and strike forces have been established, asserting a more aggressive enforcement posture for export control and sanctions violations. There is greater cooperation between the Financial Crimes Enforcement Network and the U.S. Department of Commerce on the sharing of financial data that may indicate export control or sanctions violations. There is also greater clarity on the focus of efforts targeting China, Russia and Iran.

In terms of the industries on which these efforts are focused, semiconductors, quantum computing, financial technology, shipping and artificial technology are high-profile examples. And signals from the U.S. government are clear that increased trade-related enforcement is coming.

But what should companies make of all of this?

Despite export controls and sanctions developments being regular news items, recent enforcement actions have been surprisingly infrequent. In theory, the strict liability standard makes administrative cases easier to bring than criminal cases. In criminal cases, investigations and charging decisions often take years.

Thus far in 2023, following a watershed year for sanctions targeting almost all of Russia, OFAC has announced approximately 12 civil penalties, a number of which involved sanctions programs other than Russia, and only one involving an unnamed individual.

Excluding collateral civil enforcement cases brought with DOJ cases and designations on the entities list, in 2023 the BIS has so far announced seven administrative settlements and other civil penalties — four of which were for anti-boycott violations. In total, in 2023 it issued over 130 proposed charging letters related to export and alleged anti-boycott violations.

Nevertheless, export control and sanctions enforcement is by no means a new priority for these agencies. These have been a priority for more than 15 years — since the DOJ appointed the first national export control coordinator within its former counterespionage section in June 2007. The use of administrative tools coupled with criminal enforcement goes back quite some time as well.

Messaging has also been robust throughout the years. Take, for example, the remarks of the assistant attorney general for the National Security Division in 2007 announcing the DOJ's counter-proliferation initiative: "And, we at the Department of Justice have made export control our top counterintelligence priority. In fact, we have seen a 60 percent increase in the number of export control cases filed over the past year."[1]

Because similar "tough talk" in the past has not resulted in substantial increases in enforcement matters, there are open questions regarding what this most recent reinvigorated enforcement effort actually means:

Will the DOJ's National Security Division see a material increase in voluntary self-disclosures filed on these topics? Will prosecutors in The National Security Division take the lead on prosecutions, including by using their subpoena authority? Will the type of prosecuted violations be based on more technical aspects of the Export Administration Regulations or strategically ambiguous portions of a sanctions program? What will be the role of independent monitors in these cases, given challenges that have persisted in this area on national security matters?

The overall number and quality of cases being brought is uncertain, but the DOJ and the regulatory agencies are better resourced than ever and appear to be getting more organized. Although the U.S. government's approach is still evolving, we can offer a few predictions on how the new approach to enforcement is likely to be applied going forward.

First, enforcement is likely to be rooted in highly technical underlying controls. In contrast to 2007, sanctions and export control rules have become much more complex and far-reaching, extending well beyond traditional jurisdictional constructs.

For example, there are expanded and complicated new rules governing the use of the foreign direct product rule regarding semiconductors and other items, making products that previously were outside U.S. jurisdiction potentially subject to enforcement.

On the sanctions side, routine updates and changes to various sanctions programs have expanded OFAC's "Frequently Asked Questions" to more than 1,000, as it clarifies rules targeting everything from terrorist financing to foreign corruption, underscoring how nuanced these restrictions have become.

The rules are not simple, and seldom are the hard ones intuitive. There is no question that transacting with higher-risk countries or entities carries greater risk than ever before. Russia and China remain the top enforcement priorities, but many of these rules touch every corner of the globe and cut across all industries, especially given the U.S. government's focus on sanctions and export-control evasion through third countries.

For example, the U.S. has made subject to its export controls certain items that are foreign produced but are the direct product of U.S.-origin technology or software, or are a complete plant or a major component of a plant that itself is the direct product of controlled technology.

For sanctions, the issuance of a commercial invoice for permissible services to a sanctioned party, but which has 90-day payment terms, may be considered an impermissible "extension of debt" by the Treasury and require a license.

In reality, the criminal enforcement of export controls and sanctions is not like the Foreign Corrupt Practices Act — you may know a bribe when you see one, but you would be hard-pressed, for example, to identify the misclassification of an item's export control classification number on its face.

Second, non-U.S. companies will continue to be most vulnerable to the reach and complexity of these rules because of increased efforts to identify jurisdiction and assert violations where a large degree of conduct occurred outside the U.S. There could also be an increase in multijurisdictional enforcement in conjunction with U.S. allies.

With regard to the Russia sanctions, European and U.K. allies are mostly aligned on the application of these rules and their enforcement. In recognition that these countries "have committed to implementing substantially similar export controls on Russia, Belarus, and the temporarily occupied Crimea region of Ukraine under their domestic laws," the EAR exempts them from certain restrictions with the implication that exports that would violate the EAR would be locally enforced under domestic laws.

Similarly, the Netherlands and Japan have aligned with the U.S. on export controls for cutting-edge semiconductor manufacturing equipment. Given the extraterritorial reach of U.S. controls and the emerging alignment with U.S. allies, future enforcement efforts could feature a much higher degree of international cooperation than in the past.

Third, trade agencies and the DOJ are improving the coordination of enforcement efforts between and within agencies. Multi-agency task forces — such as the Russian Elites, Proxies and Oligarchs Task Force — encourage and facilitate the sharing of information and resources.

Financial data is shared across agencies, classified intelligence is leveraged to a greater extent and components within the DOJ collaborate on these matters more than they historically have done. A new type of suspicious activity report is available to financial institutions where they suspect sanctions or export control law evasion is occurring relating to a financial transaction.

Fourth, law enforcement is clearly prioritizing export control enforcement around items, including dual-use items, that are transiting third countries and ending up in military conflicts, such as in the theater of war between Ukraine and Russia. New export controls, especially those restricting China's access to advanced semiconductors, are also aimed at slowing the development of artificial intelligence outside the U.S., because of its ability to be used to develop new weapons or military strategies.

This type of enforcement has a long history, dating back to cases prosecuting shipments involving components used in improvised explosive devices, such as U.S. v. Larijani in the U.S. District Court for the District of Columbia in 2010, and U.S. v. Yahya in the U.S. District Court for the Southern District of Florida in 2006. Not surprisingly, this very important effort continues and should continue as a priority today.[2]

Fifth, the tools available to enforcement agencies are proliferating.

For example, the Department of Commerce is now beginning to conduct investigations and explore enforcement actions under its Information and Communications Technology and Services regulations, which became effective in 2021. The Committee on Foreign Investment in the United States is also increasingly using reviews to probe companies' compliance programs and practices. It is also likely that additional regulations targeting artificial intelligence under President Joe Biden's November executive order are imminent.

U.S. prosecutors and other enforcement personnel who are taking a holistic approach have a growing number of tools with which to work, gathering information and taking action.

Sixth, future enforcement activity could be influenced by Congress and other stakeholders. Congress has become increasingly assertive in trade-related matters. For example, in 2021, the minority staff of the Senate Commerce Committee independently investigated and released a report alleging that Seagate Technology had sold disk drives to Huawei in violation of the foreign direct product rule under the EAR. The BIS subsequently conducted its own investigation, resulting in an April 2023 penalty of over $300 million.

Riding on the success of the Senate seemingly instigating an enforcement action, members of Congress — especially, for example, the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party — could make more attempts to shape enforcement policy.

Finally, there are new initiatives to trigger additional investigations. For example, in June 2022, the BIS announced a two-tiered system to fast-track minor technical violations of the EAR, and in April 2023, the agency announced a new policy under which it will treat the failure to voluntarily disclose egregious violations as an aggravating factor when assessing penalties. This carrot-and-stick approach is likely to increase the number of self-reported violations coming into the agency.

Similarly, in late 2022, the Anti-Money Laundering Whistleblower Improvement Act created whistleblower rewards for sanctions violations — although export control violations are not yet covered under the program. Coupled with a stated desire to enforce more cases against individuals, this may spur greater enforcement action, bringing to prosecutors, law enforcement and regulators greater evidence of violations by others known to these individuals.

Moreover, and by way of another example, opening investigations based on data analysis — of, e.g., IP addresses, license keys, software updates, algorithms, computer-aided design drawings, share sites, etc. — are another area to watch.

Where all this will lead in the coming years is uncertain. However, hoping for the best and preparing for the worst will be a good approach for companies to take in the event that these additional resources, in fact, lead to more aggressive enforcement that may stretch the limits of historical precedent.

Jonathan Poling is a partner at Akin Gump Strauss Hauer & Feld LLP. He previously served as a member of the DOJ foreign investment review staff at CFIUS.

Ryan Fayhee is a partner at the firm. He previously served as the DOJ National Security Division's principal official nationally overseeing sanctions and export control prosecutions.

Tyler Grove is a partner at the firm.

[1] https://www.justice.gov/archive/opa/pr/2007/October/07_nsd_806.html.

[2] United States v. Larijani, No. 1:10-cr-00174-EGS (D.D.C. 2010) and United States v. Yahya, No. 1:08-cr-20222 (S.D. Fla. 2006).