Weil

May 23, 2023

Justice Department Focus on National Security Results in First Enforcement Actions by Disruptive Technology Strike Force

A strategic shift is fully underway within federal law enforcement that seeks to use corporate criminal enforcement as a tool to advance United States national security and foreign policy objectives. Earlier this year, Deputy Attorney General Lisa Monaco publicly stated that, in the view of the Department of Justice ("DOJ"), the lines between corporate crime and national security are growing increasingly thin.[1] DAG Monaco announced a series of initiatives focused on addressing this growing trend. Among the newly announced initiatives was the formation of a joint strike force including the DOJ and the United States Department of Commerce, called the Disruptive Technology Strike Force (the "Strike Force"). Its creation introduced the DOJ's U.S. National Security Division (NSD) to the frontline of corporate criminal enforcement signaling a new era of corporate investigations in which the government plans to take aggressive action to prevent the proliferation of critical American technology to geopolitical adversaries.

This strategic shift appears to have resulted in a series of enforcement actions attributed to the Strike Force, which were announced jointly last week, on May 16, 2023, by Matthew G. Olson, Assistant Attorney General of the Justice Department's National Security Division, and Assistant Secretary for Export Enforcement at the U.S. Commerce Department, Matthew Axelrod, along with five United States Attorneys.

Building Blocks for a New National Security Enforcement Regime

The DOJ's foray into the national security arena represents a significant strategic shift in the world of corporate criminal enforcement. In the past, the DOJ's National Security Division primarily focused on terrorism-related crimes, which typically involve individuals and non-state actors. The new approach, however, focuses on state-sponsored activity, which DAG Monaco and the Director of National Intelligence have identified as the most pressing current threat to the United States. While testifying before Congress in May 2022, for example, about the most pressing threats to U.S. national security, Army Lt. Gen. Scott D. Berrier, Director of the DNI, and DNI Avril D. Haines, described an "interconnected global security environment" where the US and its allies face growing challenges from national actors such as China, Russia, and Iran." According to those officials, these nations and other non-state actors "are developing new capabilities intended to contest, limit or exceed the U.S. military advantage." The capabilities they identified exist in

conventional forces, electronic warfare, cyberspace information and space. Haines elaborated in the DNI's 2023 annual threat assessment, suggesting that technology proliferation to authoritarian regimes will contribute to increasing political instability, terrorist threats, mass migration, and other humanitarian emergencies.

The DOJ's recent policy announcements and last week's enforcement actions make clear that, along with departments and agencies that traditionally focus on national security, the DOJ is also assuming a leading role in addressing these threats. Claiming that "companies are on the front lines of today's geopolitical and national security challenges," Assistant Attorney General Kenneth Polite recently announced that the DOJ is adding 25 new prosecutors to investigate "sanctions evasion, export control violations and similar economic crimes."[2] Among the 25 new hires will be National Security Division's first-ever Chief Counsel for Corporate Enforcement. This coincides with new joint advisories with Commerce, and Treasury Departments that "inform the private sector about enforcement trends and to convey the department's expectations as to national security-related compliance."[3] In addition to sanctions evasion and export control violations, AAG Polite's remarks emphasized "a substantial investment" in the Criminal Division's Money Laundering and Asset Recovery Section (MLARS), as a significant player in these efforts.

These were only the most recent developments in a strategic shift that has gradually taken shape from the earliest days of the Biden Administration. In late 2022, for example, the DOJ and Department of Treasury had previously formed Task Force KleptoCapture to take a unified approach to addressing sanctions, export control and corruption issues.

The Initiatives Yield the First Results

Until last week, the strategic shift had largely been seen in the public speeches and policy pronouncements by government officials. Now, however, we can see a first wave of enforcement actions resulting from this government focus and investment.

On May 16, 2023, AAG Olsen announced five new enforcement actions taking aim at individuals seeking to help China, Russia and Iran gain access to sensitive U.S. technologies.

Those charged included a Greek national in the Eastern District of New York who was accused of being recruited to smuggle sensitive technologies to Russia. The individual is said to have represented to US manufacturers that he was a defense contractor for NATO and other ally countries in order to purchase U.S.-origin military and dual-use technologies via a group of companies he created in the Netherlands and Greece. According to the charging documents, however, the technology was ultimately shipped to Russia, where it was shared with nuclear and quantum research facilities as well as Russian intelligence agencies.

Similarly, in separate cases, two Russian nationals were charged in Arizona with conspiring to violate the Export Control Reform Act by sending aircraft parts to Russian airlines. In the Southern District of New York, a Chinese national was accused of participating in a scheme to use a sanctioned Chinese company to provide Iran with materials used in the production of WMDs. In both cases, the defendants are accused of having lied about who their customers were, and about where the parts would be going.

The final two cases in the Central and Northern Districts of California involved individuals who allegedly stole trade secrets belonging to their employer with the intention of sharing that technology with the Chinese Communist Party. One of the charged individuals was a former Apple software engineer who is accused of having stolen certain of Apple's source code, including plans for autonomous driving technology.

Implications

While last week's charges were all brought against individuals accused of providing military technology to hostile foreign powers, there are clear enforcement risks for the companies that manufacture these products and their component parts. Specifically, these actions underscore that companies must safeguard against; 1) disguised sales of regulated

materials to prohibited end-users; 2) unauthorized exports of dual-use technology, and 3) insider theft of trade secrets. Experience teaches that the DOJ will not stop its enforcement efforts with these individual actors, but, rather, will look to bring cases against corporate actors that fail to address these risks, much as it did in the past with respect to the Foreign Corrupt Practices Act. The activities of a corporation's agents, and any evidence of willful blindness on the part of a company's workforce are as much of a risk in the export controls and sanctions context as they have long been in FCPA context. Companies must begin to institute strict compliance structures in these domains, not only to mitigate the risk of DOJ scrutiny, but also to protect trade secrets from hostile state actors that are working proactively to obtain them.

Companies at particular risk are those that manufacture parts and components with either direct military, or dual-use applications. In announcing these enforcement actions, Assistant Secretary Axelrod, of the Department of Commerce, noted that his investigators are specifically paying close attention to sales of semi-conductors and circuits. The Strike Force is also actively monitoring companies that act as conduits for the shipment of goods throughout Asia, and they are proactively looking for purchasers that have increased – or begun – their purchases of critical technology since the recent round of U.S. sanctions were imposed on Russia in response to its invasion of Ukraine. All of these actions are evidence of a substantial – and likely sustained – effort by the U.S. government to follow-through on the policies the U.S. government has carefully instituted over the past year. Corporations must take appropriate measures to address these risks.

---

[1] Deputy Attorney General Lisa O. Monaco, Remarks at ABA's National Institute on White Collar Crime (March 2, 2023).

[2] Assistant Attorney General Kenneth A. Polite, Keynote at ABA's 38th Annual National Institute on White Collar Crime (March 3, 2023).

[3] Press Release, Department of Justice, Commerce and Treasury Issue Joint Compliance Note on Russia-Related Sanctions Evasion and Export Controls (March 2, 2023).

White Collar Defense, Regulatory & Investigations is published by the Litigation Department of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

For more information about Weil's White Collar Defense, Regulatory & Investigations practice, please contact:

Sarah Coyne (Practice Co-Head, NY)	View Bio	sarah.coyne@weil.com	+1 212 310 8920
Daniel L. Stein (Practice Co-Head, NY)	View Bio	daniel.stein@weil.com	+1 212 310 8140
Steven A. Tyrrell (Practice Co-Head, DC)	View Bio	steven.tyrrell@weil.com	+1 202 682 7213