Updates
October 02, 2024
Strike Force Cases Highlight Focus on National Security Priorities and Need for Strengthened Cybersecurity

The U.S. Department of Justice (DOJ) announced criminal charges in five cases in connection with the Disruptive Technology Strike Force (Strike Force) on September 16, 2024. Launched in February 2023, the Strike Force is jointly led by DOJ's National Security Division and the Department of Commerce's Bureau of Industry and Security (BIS) and involves five agencies across the government, multiple U.S. attorneys' offices, and local law enforcement. The Strike Force, according to Assistant Attorney General Matthew G. Olsen, is tasked with stopping the transfer of "sensitive, cutting-edge technologies to Iran, China, and Russia" and preventing such technologies from being used in military capabilities and other programs that enable human rights abuses in these countries. The Strike Force is a prime example of the U.S. government's attention to efforts by strategic adversaries to commercially acquire American products and technology. Companies—including startups, small companies with access to strategic technology, and research institutions such as universities—should take steps to ensure their compliance controls are well-tailored to their risks in relation to export control and sanction evasion. The breadth of the defendants' targets and techniques that these Strike Force actions highlight also merits attention, as the defendants leveraged the openness of the American economy and research enterprise.

The Strike Force's Efforts and Recent Cases

In the year and a half since its launch, the Strike Force's work has led to charges unsealed against 34 defendants in 24 cases, reflecting the considerable resources dedicated to the Strike Force and the emphasis that federal agencies have placed on controlling the flow of critical technologies out of the United States. The Strike Force's cases involve export control violations, smuggling, trade secrets theft, and other charges associated with actors with connections primarily to Russia, China, and Iran.

The latest cases reflect the priority that U.S. enforcement agencies are placing on prosecuting export control evasion and, more broadly, white-collar crimes implicating national security priorities. The five most recent

cases include the following allegations:[1]

- *United States v. Postovoy*, charging a Russian citizen living in the United States for conspiring to violate U.S. export controls by procuring and illicitly exporting from the U.S. to Russia microelectronic components with military applications in unmanned air vehicles (UAVs) or drones. The Russian citizen used a web of companies based in Hong Kong to purchase microelectronics from U.S.-based distributors and ultimately transshipped those items to Russia by submitting false information on export-related documents and misstating the true end users/end destinations of the items.
- *United States v. Song Wu*, charging a China-based employee of a Chinese government-owned defense company with wire fraud and aggravated identity theft. The defendant used "spear phishing" email campaigns to impersonate U.S.-based researchers and engineers to obtain restricted computer software and source code for use in developing Chinese industrial and military applications, including in developing advanced tactical missiles.
- *United States v. Bhambhan and Teslenko*, charging a Massachusetts resident and a Russian national for conspiracy to export laser welding machines to a Russian state-owned plant located in Russia by falsifying export documentation to conceal the end user of those machines. The indictment stated that the machines were intended for use in the Russian nuclear weapons program.
- *United States v. Goodarzi*, charging a dual U.S. and Iranian citizen who resides in the United States for smuggling parts and components used in producing UAVs and other manned aircraft from the United States to Russia. Court documents indicate that the defendant did not have a license to export those parts but nonetheless purchased U.S.-origin aircraft components from U.S.-based suppliers and exported them to Iran. Court documents also alleged that the defendant concealed aircraft parts in his luggage when traveling to and from Iran multiple times a year.
- *United States v. Nader*, charging a U.S.-Iranian dual national residing in the United States for procuring U.S.-manufactured aircraft components (including components used in military aircraft) and attempting to export those components to Iran for use on Iranian military aircraft, including the F-4 fighter jet. The defendant used his California-based company to approach U.S.-based suppliers and obtain the components as part of the conspiracy to export those components to Iran.

Takeaways for Businesses

Each of these cases highlights the Strike Force's focus on and capabilities in pursuing crimes at the intersection of business and national security. They also highlight the increasing application of the "whole of government" model to national security crimes involving and affecting corporate America, particularly relating to the development and procurement of critical technologies. This emphasis will likely increase in the future, as U.S. enforcement agencies have explicitly stated that enforcement of national security laws that directly involve corporations and the private sector (*i.e.*, export controls) is now the top U.S. enforcement priority. The recently announced charges are part of a broader trend in which the laws and regulations associated with cross-border trade, financial transactions, and data flows are vastly expanding while the U.S. government intensifies enforcement resources dedicated to national security priorities. These trends include the Corporate Transparency Act; anti-money laundering obligations targeting the real estate and investment sectors; expansive new foreign investment restrictions and export controls; Task Force KleptoCapture; and several new whistleblower reward initiatives, among others.

For businesses in the technology space that deal with critical technologies that have military or intelligence applications—or, at the very least, are potentially "dual use" products (products that have both civilian and military applications)—it is essential to vet and screen individuals and entities that seek access through such means as employment, collaboration, vendor agreements, investment, and purchasing. As the recently announced Strike Force cases highlight, even if a business or individual represents a U.S.-based entity when purchasing a product, reliance on such representations may not be sufficient. Companies should take a risk-based

approach to vetting even their U.S. counterparties and ensure they understand their customer's customer in circumstances involving controlled technologies and goods. And, as maintaining information security grows more important and difficult each day, technology companies—particularly those that deal with technologies and/or computer source code that could be applied to military components—must be ever diligent in maintaining strong cybersecurity plans to safeguard against unauthorized attempts to extract information and technologies that may find themselves in the wrong hands.

The upshot is that technology companies can expect that government agencies will continue to focus on how critical technologies are managed, maintained, and transmitted, and companies should continue to implement and strengthen their vetting and screening programs to prevent any unauthorized transmission or export to unintended end users. For matters related to export controls, financial sanctions, and information security, companies should consult with experienced counsel.

Endnote

[1] Criminal charges are only allegations at this stage.

Authors

Explore more in

International Trade | Financial Transactions | Privacy & Security | White Collar & Investigations | Data Security Counseling and Breach Response

Related insights

Update

President Trump Creates "Make America Healthy Again" Commission

Update

FERC Meeting Agenda Summaries for February 2025