NOW & NEXT

Government Investigations & White Collar Alert

FEBRUARY 17, 2023

DOJ creates Disruptive Technology Strike Force

By Christopher D. Grigg, Alexandra López-Casero, and David F. Crosby

Here's what businesses and research institutions can expect in the wake of DOJ's announcement of its new initiative to combat the illicit transfer of advanced technologies to foreign adversaries.

What's the Impact?

- The federal government is ramping up its policing of advanced technologies in computing, manufacturing, and biosciences.
- A newly announced strike force will leverage powerful investigative tools to pursue wrongdoers and hold them accountable.
- Organizations in advanced technology fields should take stock and invest in export compliance programs.

Speaking in London on Thursday, Feb. 16, Deputy Attorney General Lisa O. Monaco announced the creation of a new strike force as part of a joint effort led by the U.S. Department of Justice (DOJ) and the Commerce Department "to target illicit actors, enhance public-private partnerships to harden supply chains, and identify early warning of threats to our critical assets, like semiconductors." According to a DOJ press release, the newly formed Disruptive Technology Strike Force will leverage the robust capabilities of the United States' most powerful export enforcement agencies — the FBI, Department of Commerce, and Homeland Security

Investigations (HSI) — and federal prosecutors from 14 U.S. Attorney's Offices across the country to "attack tomorrow's national security threats today."

Key line of attack: Increased export enforcement

Led by Assistant Attorney General for National Security Matthew G. Olsen and Assistant Secretary for Export Enforcement Matthew Axelrod of the Commerce Department's Bureau of Industry and Security (BIS), the Disruptive Technology Strike Force "will focus on investigating and prosecuting criminal violations of export laws [and] enhancing administrative enforcement of U.S. export controls" in a variety of fields, including "supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences." Technologies in these fields "have important commercial uses" but, in the wrong hands, can threaten national security, especially when nation-state adversaries use them for malign purposes.

Thursday's announcement is the latest signal of a growing trend: The United States is intensifying its policing of critical technologies to make it harder for adversaries to obtain them. To that end, the strike force will use all available resources, including partnering with the private sector, working with foreign law enforcement agencies, and employing advanced data analytics and "all-source intelligence to build investigations." To ensure its own personnel are well-equipped and well-informed, the strike force will implement regular trainings and strengthen its ties to the United States Intelligence Community.

What to expect: Increased federal scrutiny and engagement

Businesses and research institutions in advanced technology fields, especially those working with foreign partners, should expect increased scrutiny of their practices and increased engagement with investigators. Engagement can take several forms, including requests for interviews, visits to offices and facilities, and document requests.

A federal agent's visit or request for information does not necessarily mean that a particular business or institution is itself under suspicion — in some instances, investigators merely seek to learn more about a particular technology or industry. But in instances of suspected wrongdoing, strike force agents and prosecutors will bring to bear a powerful set of tools to investigate those responsible. Those tools range from document requests and administrative subpoena powers wielded by BIS and HSI, to the FBI's national security authorities, and ultimately to federal prosecutors' abilities to obtain compulsory process such as grand jury subpoenas, pen registers, court orders for historical electronic data, search warrants, and wiretaps.

The strike force will use its combined capabilities to investigate suspected violations of United States export controls found in laws and regulations such as the Export Control Reform Act, International Emergency Economic Powers Act, Export Administration Regulations, various sanctions regulations administered by the Treasury Department, and — in cases involving defense articles and technical data — the Arms Export Control Act and International Traffic in Arms Regulations. Violations of these laws and regulations can result in public allegations of wrongdoing; administrative fines; loss of export privileges; debarment from contracting with the

federal government; asset forfeiture; and, in the most serious cases involving willful violations of the law, criminal prosecutions leading to imprisonment, fines, and restitution orders.

Often, export investigations unearth violations of the unlawful export information statute (for failure to file or filing false electronic export information) and ancillary crimes such as wire fraud and money laundering, each of which carries its own substantial criminal penalties. The strike force is expected to vigorously pursue prosecutions of all such offenses, using the full array of criminal arrows in its quiver to target bad actors and disrupt illicit conduct.

What to do: Take stock and invest in compliance

Businesses and research institutions in advanced technology fields understandably might not focus on export compliance, but Thursday's announcement makes clear that they should, particularly because many of the advanced technologies (listed below) are becoming more commonplace in everyday business activities. Effective compliance is the best way to avoid the potential consequences of an administrative or criminal enforcement action. It starts with a commitment by senior leadership to a culture of compliance and the willingness to back that commitment with sufficient support and resources.

While the press release did not specifically identify the advanced technology fields involved, we anticipate, based on prior pronouncements by the Biden Administration, that these will likely include advanced computing, supercomputing, quantum computing, artificial intelligence and machine learning, microelectronics, semiconductors in the advanced technology nodes, supply chain technologies, biotechnology and biomanufacturing, advanced clean energy technologies, climate adaptation technologies, and advanced agricultural technologies. And we would expect this list to expand over time.

Organizations, especially those in these and other advanced technology fields, should candidly assess whether and to what extent export controls apply to their technologies and identify which federal agencies administer those controls. For example, the rules for technologies controlled by the Export Administration Regulations can differ dramatically from those that apply under the International Traffic in Arms regulations. Organizations must appreciate the difference and tailor their behavior accordingly.

Know-your-customer obligations are familiar and necessary for export compliance, but they are not sufficient. Organizations must also know themselves. Preventing the unauthorized release of controlled technology to foreign nationals (whether located in the United States or abroad), prohibited end-users, prohibited destinations, and for prohibited end-uses is impossible without first taking stock of supply chains, internal operations and data security practices, and distribution channels. Taking stock will also enable organizations that employ or frequently interact with foreign nationals to create an effective technology control program that accounts for physical and information security measures, personnel screening, and workforce training. It will also help determine when to apply for necessary licenses.

Regardless of which export control regime applies, effective compliance programs must ensure that organizations abide by the applicable and often-detailed export documentation and record retention requirements. Failure to comply with those requirements can itself constitute a violation of the export control laws. Organizations that don't invest in compliance, train their workforce, and audit their own practices will learn that the hard way when strike force agents serve document requests and administrative subpoenas.

Fortunately, abundant resources are available to help businesses and research institutions build and maintain effective compliance programs. Experienced compliance and enforcement counsel can help guide organizations through that process.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Christopher D. Grigg
213.629.6134
cgrigg@nixonpeabody.com

Alexandra López-Casero
202.213.0171
alopezcasero@nixonpeabody.com

David F. Crosby
617.345.1264
dcrosby@nixonpeabody.com