UNITED STATES DEPARTMENT OF COMMERCE
Assistant Secretary for Export Enforcement
Washington, D.C. 20230

Export Enforcement: 2024 Year in Review

The men and women of Export Enforcement work tirelessly to help safeguard our collective national security. From degrading the Russian war machine to stopping the People's Republic of China (PRC) from acquiring advanced U.S. technology, our efforts impose costs on adversaries and degrade their battlefield capabilities. Along with our law enforcement partners, we are the tip of the spear when it comes to keeping our country's most sensitive technologies out of the world's most dangerous hands.

To protect our national security over the past calendar year, we:

Continued to deliver concrete results through the Disruptive Technology Strike Force, which protects U.S. advanced technologies from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran. More specifically, we**:**

- Expanded the geographical reach of the Strike Force from 14 to 17 locations, with new cells in Texas, Georgia, and North Carolina, and added the Defense Criminal Investigative Service (DCIS) as a Strike Force law enforcement partner, alongside BIS, DOJ, FBI, and HSI.
- Brought 15 criminal cases charging sanctions and export control violations, smuggling conspiracies, and other offenses related to the transfer of sensitive information, goods, and military-grade technology to the PRC, Russia, and Iran, for a total of 26 criminal cases since the Strike Force's inception;
- Imposed a $5.8 million administrative penalty on TE Connectivity after its voluntary self-disclosure of the unauthorized export of low-level items to parties tied to PRC military electronics programs; and
- Nominated 22 parties to the Entity List for acquiring or attempting to acquire U.S.-origin items to enhance PRC quantum capabilities.

Took impactful enforcement action against significant national security threats. Alongside DOJ and our other law enforcement partners, we:

- Targeted illicit Russian procurement networks, including:
  - Obtained the guilty plea of a defendant who played a critical role in exporting to Russia sensitive electronic components used in the development of nuclear and hypersonic weapons;
  - Indicted several Russian nationals and extradited a Russian-German national from Cyprus on charges of procuring large quantities of microelectronics for the Russian defense base;
  - Obtained a guilty plea from a New York man for his role in an illicit procurement scheme to ship U.S.-made electronic components to companies affiliated with the Russian military;
  - Obtained guilty pleas from a Canadian national, a U.S. national, and a Russian-Canadian national for their roles in sending components used in drones and missile systems to sanctioned entities in Russia;
  - Arrested a defendant in Los Angeles on charges he conspired to transfer hundreds of thousands of semiconductors to sanctioned entities tied to Russian military and intelligence agencies;
  - Imposed a $180,000 mitigated penalty against a New York company for exports to Russia of solder materials used in electronics manufacturing; and
  - Imposed a $3.3 million civil penalty on a California company for exporting transistors and related products, including Common High Priority List (CHPL) items, to Russia.

- Held accountable those sending sensitive technology to nation-states like China and Iran:
  - Obtained a guilty plea from a Chinese citizen for illegally exporting a semiconductor manufacturing machine to an Entity-Listed company in China;
  - Arrested a Chinese national for alleged theft of artificial intelligence-related trade secrets from Google;

- Arrested a California man on charges of stealing trade secrets used by the U.S. to detect nuclear missile launches and track ballistic and hypersonic missiles, potentially for the benefit of the PRC;
- Imposed a $500,000 mitigated penalty against GlobalFoundries for shipping $17 million worth of semiconductor wafers to a Chinese company on the Entity List;
- Charged four Chinese nationals with conspiring to smuggle U.S. parts to Iranian entities affiliated with the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Defense and Armed Forces Logistics;
- Arrested a U.S.-Iranian national on charges of illegally exporting aircraft components to Iran, some of which could be used on the F-4 fighter jet operated by Iran's armed forces; and
- Arrested a defendant for providing material support to the IRGC and allegedly procuring sensitive U.S. technology that was used in IRGC military drones, one of which killed three U.S. servicemembers.

- Took other significant enforcement actions:
  - Denied for a period of three years the export privileges of USGoBuy LLC, a package forwarding company, due to continued export control violations and failure to address past compliance deficiencies;
  - Obtained a sentence of 70 years in prison for a Pennsylvania man who tortured an Estonian citizen in 2015 and illegally exported weapons parts to Iraq;
  - Seized a $13 million Dassault Falcon 900EX aircraft owned for the benefit of Nicolás Maduro Moros;
  - Forfeited a Boeing 747 cargo plane previously owned by Mahan Air, a sanctioned Iranian airline;
  - Arrested two defendants on charges of exporting millions of dollars' worth of grenade launchers, Stinger missile systems, and other controlled items to South Sudan in support of a planned coup attempt;
  - Obtained a guilty plea from the self-described "King" of a notoriously violent Haitian gang for his role in a gunrunning conspiracy that smuggled firearms to Haiti;
  - Participated in the disruption of a botnet—likely the world's largest ever—which infected over 19 million IP addresses and facilitated cyber-attacks, export violations, and billions of dollars of fraud; and
  - Arrested an Ontario man on charges of obtaining firearms, ammunition, and other military-grade equipment with the intention of shipping them to North Korea for military use.

Further strengthened our enforcement program and policies:

- Amended our administrative penalty guidelines and our voluntary self-disclosure (VSD) guidelines to more properly reflect current practices and policy;
- Hired BIS's first-ever Chief of Corporate Enforcement to serve as the primary interface between BIS agents, BIS enforcement attorneys, and DOJ prosecutors to facilitate resolution of corporate investigations; and
- Established the Commerce Screening System to automate the screening of foreign entities on 100% of export license applications against intelligence holdings, replacing what was an entirely manual process.

Designed innovative strategies to help reduce the flow of high-priority dual-use items to Russia:

- For the first time ever, placed addresses on the Entity List – 16 addresses in Hong Kong and Turkey housing hundreds of shell companies that diverted more than $130 million in high-priority items to Russia;
- Sent more than 40 "red flag" and "supplier list" letters to U.S. companies identifying foreign parties that pose diversion risks;
- Issued industry guidance outlining the differences between "red flag," "supplier list," and "is informed" letters; and
- Recommended a new best practice that exporters of high-priority items to Russia screen transaction parties using online resources made newly available by the Trade Integrity Project.

Developed key partnerships with the interagency, industry, and foreign governments:

- With the assistance of foreign governments, completed over 1,440 end-use checks in 60 countries;
- Issued new freight forwarder guidance providing an overview of the roles, responsibilities, and best practices for freight forwarders in export transactions;
- Published guidance for financial institutions containing best practice recommendations for complying with the Export Administration Regulations, including General Prohibition 10;

- Updated "Don't Let This Happen to You!," our compendium of criminal and administrative case results;
- Published a tri-seal advisory with DOJ and Treasury on export control obligations of non-U.S. entities;
- Celebrated the one-year anniversary of the Disruptive Technology Strike Force with a convening in Phoenix, Arizona that included law enforcement, industry, academia, and Ukrainian government partners;
- Published, for the first time ever, joint guidance with the G7 on preventing Russian export control evasion;
- Formally established the Disruptive Technology Protection Network, a partnership with Japan and South Korea to exchange enforcement information and best practices;
- Hosted the second annual Export Enforcement Five Conference to expand export enforcement collaboration among the United States, Australia, Canada, New Zealand, and the United Kingdom; and
- Signed individual bilateral agreements with the Australian, Japanese, South Korean, and Swiss governments to facilitate law enforcement cooperation and information sharing.

Provided new resources to the academic community to assist their export compliance efforts:

- Hosted webinars on identifying red flags and fundamental research for over 50 universities;
- Expanded our Academic Outreach Initiative, which was established in 2022 to help academic institutions protect themselves from overseas threats and ensure research security, from 29 to 40 universities;
- Issued a compendium of export compliance resources for academic institutions; and
- Analyzed trends in VSDs filed by academic institutions to help focus their export compliance efforts.

Further strengthened our antiboycott enforcement efforts, including by creating a new Boycott Requester List:

- Established an innovative Boycott Requester List to help U.S. persons better identify reportable boycott-related requests they may receive;
- Removed more than 40 companies from the Requester List for certifying that they have changed their behavior and have stopped making boycott requests of U.S. persons;
- Published an advisory related to Türkiye's announced suspension of imports from Israel; and
- Imposed a total of nearly $400,000 in penalties on 4 companies to resolve alleged antiboycott violations.

Successfully placed numerous parties on the Entity List for actions contrary to our national security and foreign policy. Through the established interagency process, nominations from Export Enforcement resulted in more than 340 parties from China, Russia, Iran, and other countries being added to the Entity List.