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

# Export Enforcement: 2023 Year in Review

At no point in history have export controls been more central to our collective security than right now. Advances in science and technology are poised to define the geopolitical landscape of the 21st century, with disruptive technologies like artificial intelligence and quantum computing at the forefront. Export Enforcement's work to protect these advanced technologies from falling into the wrong hands is critical.

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

**Launched the Disruptive Technology Strike Force with the Department of Justice (DOJ) to protect U.S. advanced technologies from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran.** The Strike Force brings together experienced agents and prosecutors in fourteen locations across the country, supported by an interagency intelligence effort in Washington, D.C., to pursue investigations and take criminal and/or administrative enforcement action as appropriate. Since its inception, the work of the Strike Force has resulted in numerous indictments, temporary denial orders (TDOs), and Entity Listings.

**Took enforcement action against significant national security threats, including the highest number ever of convictions, TDOs, and post-conviction denial orders.** Together with FBI, HSI, ATF, and other law enforcement partners, we:

- Imposed the largest standalone administrative penalty in BIS history – a $300 million penalty against Seagate and Seagate Singapore International Headquarters Pte. Ltd. of Singapore related to their continued shipment of millions of hard disk drives to Huawei even after their two main competitors stopped shipping due to the foreign direct product rule.
- Announced the initial round of Disruptive Technology Strike Force cases with the filing of criminal charges by five different U.S. Attorney's offices in cases involving China, Russia, and Iran. Also issued a related TDO suspending the export privileges of five entities and two of the charged defendants for diverting civilian aircraft parts to Russia.
- In coordination with DOJ, charged a Belgian national for a scheme to export military-grade technology, including accelerometers and missile components, to China and Russia. At the same time, the defendant was arrested by Belgian authorities and he and his companies were added to the Entity List by BIS and to the Specially Designated Nationals and Blocked Persons List by the Department of the Treasury's Office of Foreign Assets Control (OFAC).
- Worked with DOJ to bring eight separate indictments charging 14 people for their role in procuring items for the Russian military and Russian security service, including:
    - Two Kansas men for an alleged scheme to illegally export sophisticated avionics, one of whom subsequently pleaded guilty;
    - A Russian national for allegedly supplying electronic devices used for counterintelligence operations to the Federal Security Service of the Russian Federation (FSB) and North Korea; and
    - Three Russian nationals for allegedly using companies in Brooklyn to unlawfully purchase millions of dollars' worth of dual-use electronics on behalf of end users in Russia, including companies affiliated with the Russian military.
- Worked with DOJ to obtain a guilty plea from a program administrator for a NASA contractor who secretly funneled sensitive aeronautics software to Beihang University, which is on the Entity List for its involvement in developing Chinese military rocket systems and unmanned air vehicle systems.
- Imposed a $2.77 million penalty on a 3D printing company related to its sending export-controlled blueprints for aerospace and military electronics to China.

- With DOJ, announced two different seizures of 16 website domains associated with Lebanese Hizballah.
- In coordination with OFAC, imposed a $3.3 million combined penalty against Microsoft Corporation for alleged and apparent violations of U.S. export controls and sanctions laws, including violations involving Russia, Cuba, Iran, and Syria.
- Helped convict a Pennsylvania man of torture – the second time an American has been convicted of the crime since the federal torture statute went into effect in 1994.
- With DOJ, obtained a guilty plea from a Rhode Island man for purchasing "ghost gun" kits and machining them into working firearms, which were unlawfully exported to the Dominican Republic.
- Worked with DOJ to obtain a guilty plea from Broad Tech System for its involvement in a scheme to illegally export chemicals to a Chinese company that has ties to the Chinese military.

**Strengthened our enforcement policies to help keep the most critical U.S. technology out of the most dangerous hands:**

- Clarified our voluntary self-disclosure (VSD) policy to specify that if a company knows of a significant potential violation and affirmatively decides not to divulge it, that lack of disclosure will be an aggravating factor in any subsequent penalty calculation should the violation later be discovered.
- Announced that when a party informs us about another party's conduct and that information allows us to take enforcement action, we will consider it "extraordinary cooperation" and treat it as a mitigating factor if the notifying party engages in prohibited conduct in the future.
- Revised the categories of what we measure internally – our metrics – to better reflect and further our prioritized enforcement efforts against the most pressing national security threats.
- Amended our regulations to permit the renewal of certain TDOs for a period of one year, rather than just 180 days, where a party has engaged in a pattern of repeated, ongoing and/or continuous apparent violations of the EAR.
- Joined DOJ in proposing an amendment to the federal Sentencing Guidelines to clarify that §2M5.1 unambiguously encompasses the full spectrum of national security related controls.

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

- With the assistance of foreign governments, completed over 1,500 end-use checks – our most ever in a single year.
- Issued a joint alert with FinCEN containing the first-ever key term for financial institutions to use when filing Suspicious Activity Reports (SARs) for global export evasion.
- Issued a FinCEN/BIS joint alert regarding Russian evasion of U.S. export controls, detailing evasion typologies, introducing nine new high priority Harmonized System (HS) codes to inform U.S. financial institutions' customer due diligence, and identifying additional transactional and behavioral red flags.
- Published "best practice" guidance for industry related to the nine highest-priority HS codes sought by Russia for its missile and unmanned aerial vehicle (UAV) programs and provided a model customer certification form.
- For the first time ever, issued tri-seal compliance notes with DOJ and Treasury on Russian evasion tactics and voluntary self-disclosures.
- Established export enforcement coordination mechanisms with export enforcement partners in Australia, Canada, New Zealand, and the United Kingdom (i.e., the "Export Five" or "E5") and G7 counterparts.
- Published joint guidance from the E5 for industry and academia addressing high priority items needed by Russia's military and explaining how exporters can identify Russian diversion pathways.
- Implemented a new data sharing arrangement with the European Anti-Fraud Office (OLAF) to allow closer coordination on export enforcement.
- Issued guidance to industry with the Departments of Justice, Treasury, and State on Iran's procurement, development, and proliferation of UAVs and on Iran's ballistic missile procurement activities.

- Issued a "Know Your Cargo" joint compliance note with the Departments of Justice, Homeland Security, State, and Treasury focused on maritime and other transportation industries.
- Expanded our Academic Outreach Initiative to 29 institutions to help academic institutions maintain an open, collaborative research environment in a way that also protects them from national security risk.
- Signed a memorandum of understanding with OFAC formalizing our close coordination and partnership.
- Created an Export Enforcement listserv, so that industry and academia can sign up to receive a notification whenever something enforcement-related gets posted to the BIS website.

**Expanded and enhanced our antiboycott enforcement efforts to ensure that U.S. companies are not used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel:**

- Amended the Boycott Reporting Form to include the name of the specific party making a boycott-related request, which will help the Office of Antiboycott Compliance investigate such requests.
- Published policy statements on both the Department of Commerce's and the broader U.S. Government's acquisition websites clearly articulating the requirements of the antiboycott regulations and their applicability to government contracts.
- Imposed over $425,000 in penalties on companies for alleged violations of the antiboycott regulations, including $283,500 against Regal Beloit FZE, a foreign subsidiary of Regal Beloit America, Inc., to resolve 84 violations related to antiboycott requests from a Saudi Arabian customer.

**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 the addition to the Entity List of more than 465 parties from China, Russia, Iran, and elsewhere.