March 2023 | Vol. 37, No. 3

# EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:


- MORE DATA EXPORT ENFORCEMENT
- DISRUPTIVE TECH TASK FORCE
- BIS / DOJ/ OFAC COLLABORATE
- CHINA'S CCIC COURT
- ADEYEMO: US OR THEM


# Congress Tackles Trade

*Bipartisan Consensus on Trade Security*

# RED FLAGS

## for Export Compliance

**Things that should alert you to potential violations of the Export Administration Regulations.**

- ✓ The customer or its address is similar to one of the parties found on the Commerce Department's list of denied persons.
- ✓ The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- ✓ The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- ✓ The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- ✓ The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- ✓ The customer has little or no business background.
- ✓ The customer is unfamiliar with the product's performance characteristics but still wants the product.
- ✓ Routine installation, training, or maintenance services are declined by the customer.
- ✓ Delivery dates are vague, or deliveries are planned for out of the way destinations.
- ✓ A freight forwarding firm is listed as the product's final destination.
- ✓ The shipping route is abnormal for the product and destination.
- ✓ Packaging is inconsistent with the stated method of shipment or destination.
- ✓ When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport.

**Reading for Export Compliance**
**The Export Practitioner**

**www.exportprac.com**

EP
THE EXPORT PRACTITIONER™
MARCH 2023 | VOL. 37, NO. 3


FEATURES

# Congress Tackles Trade

•**Congress Bulls:** Bipartisan Trade Legislation | **4**
•**Axelrod and Kendler:** Call for Global Coordination | **6**
•**Adeyemo:** Respect Sanctions or Lose Access | **8**
•**BIS/DOJ/OFAC:** Third Countries Under Scrutiny | **10**

## POLICY

**Foreign Affairs** Chair Raps Licensing Regime | **13**
**China Belt & Road Court** (CICC) Report | **13**
**CFIUS:** Five Eyes Exemptions Complete | **14**
**FISA:** Section 702 Renewal Kickoff | **14**

## ENFORCEMENT

**Honeywell:** Distributor Arrested for Russia Sales | **15**
**3D Systems:** $12.75 MM Fine for Data Exports | **15**
**Ericsson:** Buries the Hatchet on DPA Violations | **16**
**Petrobras:** Connecticut Oil Traders Indicted | **17**
**FSB:** Russian Charged as Procurement Agent | **17**

## SANCTIONS

**Treasury:** Flags Emirates as Sanctions Buster | **18**
**Russia** Aluminum Tariffs | **19**
**Ukraine** Grid Assistance | **19**
**Low Tech EAR99** Rules Expanded for Russia | **19**
**Briefs:** OFAC, BIS, China, KleptoCapture | **20**

## EXPORT CONTROLS

**Disruptive Technology:** Enforcement Task Force | **23**
**China:** Expands Export Controls | **23**
**Briefs:** Macau Chips, CFIUS, Wassenaar | **23**

**ON THE COVER:** Cherry blossoms and the Thomas Jefferson Memorial in Washington, D.C. (CREATIVE COMMONS: RON COGSWELL)

**The Export Practitioner**
www.exportprac.com

**Mailing Address:** P.O. Box 7592, Arlington, VA 22207
**Telephone:** 301-460-3060
**E-Mail:** info@exportprac.com

Published monthly by Gilston-Kalin Communications, LLC.

**Editor:** Frank Ruffing,
**Advisory Editor:** Mary Berger
**Editor Emeritus:** Sam Gilston
**Geneva Editor:** Devarakonda Ravi Kanth
**Design and Production:** Creative Circle Media Solutions

**Annual Subscription:**
Domestic & International, $849
Site and Enterprise licenses available.
POSTMASTER: Send Address Changes to the Above Address.


ISSN 1087-478K

**The United States Capitol in Washington, D.C.**

CREATIVE COMMONS: JMARCOSNY

# Congress Bulls in China Shop

The first hearing held by the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party capped a month of activity by House lawmakers focused on China, including approval of a raft of China-focused bills by the Financial Services and Foreign Affairs Committees.

## Gallagher Committee Launches

Members of the newly-created Select Committee on China spent their inaugural session calling for bipartisan support to counter the economic and national security threats posed by China.

**Rep. Mike Gallagher (R-Wisc)**, chair of the Select Committee, urged his members to act "with a sense of urgency" and on a bipartisan basis in arriving at proposals to counter Beijing.

"We may call this a strategic competition, but it's not a polite tennis match," he said. "This is an existential struggle over what life will look like in the 21st century — and the most fundamental freedoms are at stake."

Over the course of the three-hour hearing, lawmakers from both sides of the political aisle raised numerous concerns over China's behavior and policies — and its potential aggression toward Beijing.

Many of the issues they raised are already the subject of legislation, like limiting or prohibiting Chinese investment in US agricultural land and companies. Similarly, questions were raised about whether there should be restrictions on US investment in China, particularly in the technology sector.

China's unfair trade practices were raised, with several members from both sides of the

political aisle suggesting the time has come to revoke China's permanent normal trade relations status.

## McCaul Continues BIS Drumbeat

**Committee Chairman Michael McCaul (R-Texas)** commended the Administration for recently-imposed export controls on semiconductors and semiconductor. But he sharply criticized the Commerce Department's Bureau of Industry and Security, saying that BIS "continues to grant licenses that allow critical US technology to be sold to our adversaries – even those it's designated as threats to national security."

He charged that in one recent six-month time period, BIS approved licenses worth $60 billion to. Huawei and $40 billion to SMIC, which are both on the Entities List. "If BIS continues to mindlessly green light sensitive technology sales, the CCP has proven they will use our own inventions against us," he said.

Mr. McCaul said he is ready to work with the Administration to beef up US export controls.

## Raft of China-Focused Bill Approved

The House Financial Services Committee approved a long list of bills, mostly aimed at sanctioning China if it takes any military action against Taiwan. The measures were passed with bipartisan support, paving the way for action on the House floor.

Addressing the economic and national security risks posed by China is high on the House's priority list for the 118th Congress. The first hearing held by Financial Services this year was on China.

"We know China is not an ally or a strategic partner. They are a competitor," **committee chairman Patrick McHenry (R-NC)** said before the mark up.

**Ranking Democrat Maxine Waters (Calif)** also endorsed the China bills. But she called the measures "modest efforts to hold China accountable," arguing that the biggest threats to the US economy are a possible default on US debt and inflation.

## Bills approved by the committee include:

• The "Taiwan Conflict Deterrence Act of 2023 (HR 554) to disincentivize Chinese aggression towards Taiwan by publishing the assets of top Chinese leaders, as well as cutting them and their family members off from financial services, if Beijing acts against Taiwan.

• The "*Taiwan Non-Discrimination Act of 2023*" (HR 540) to require the United States to advocate for Taiwan's membership at the International Monetary Fund.

• The "*Chinese Currency Accountability Act of 2023*," (HR 510) to prevent the Chinese Communist Party from coopting critical international institutions like the International Monetary Fund by requiring the Treasury Secretary to oppose an increase in the weight of China's renminbi in the basket of currencies determining the value of Special Drawing Rights.

• The "*China Exchange Rate Transparency Act of 2023*," (HR 839) to protect global market participants from the CCP's exploitative practices by requiring the US Director at the International Monetary Fund to advocate for greater transparency in China's disclosure of its exchange rate policies.

• The "*PROTECT Taiwan Act*," (HR 803) to help isolate the CCP from the international financial system by directing the Federal Reserve, the Secretary of Treasury and the Securities and Exchange Commission to exclude representatives from the People's Republic of China from proceedings of various international financial groups and organizations in the event of an invasion of Taiwan.

• The "*Securing America's Vaccines for Emergencies (SAVE) Act of 2023*," (HR 555) to end US over-reliance on adversarial governments for medical supplies during an emergency by bolstering and diversifying existing supply chains through the Defense Production Act.

• The "*China Financial Threat Mitigation Act of 2023*," (HR 1156) to promote American financial resiliency by requiring the Treasury Secretary to report on global economic risks emanating from the Chinese financial sector.

*This is an existential struggle over what life will look like in the 21st century – and the most fundamental freedoms are at stake*

**Rep. Mike Gallagher** (R-Wisc)

*Unlike other geopolitical challenges, export enforcement cannot be effective unless there is a coordinated global effort.*

**Matthew Axelrod,** Assistant Secretary for Export Enforcement

# Axelrod Touts Enforcement Collaboration, Expansion

**Assistant Secretary of Commerce for Export Enforcement Matt Axelrod** spoke to the 12th Annual Forum on U.S. Export & Re-export Compliance for Canadian Operations Jan 31 in Totonto. The following has been edited for brevity.

**"Simply put, export controls are a shared endeavor.** And when it comes to export enforcement, cooperation is critical to ensure our shared security. Countries implementing multilateral export control regimes have long known that such controls are critical to the world's safety, and most effective when widely implemented across the globe. But our current geopolitical challenges, the increasingly rapid development of technology with the potential to provide asymmetric military advantage, and the countless ways in which the world is now interconnected, have raised the prominence and impact of export controls in unprecedented ways

**And that means that the importance of export enforcement has risen in unprecedented ways as well.** It's not sufficient for likeminded countries just to have parallel controls on paper. It's critically important, but it's not sufficient. We also need to ensure a common commitment to effective implementation and enforcement of those controls. In other words, export enforcement must be a shared focus across the globe. Strong multilateral export enforcement coordination is essential to keeping the world safe. All likeminded countries should be looking to build their export enforcement capacity, both individually and collectively.

But given the increase in security risk that advanced technologies — such as quantum computing, hypersonic weapons, and unmanned aerial vehicles — now pose, **we need all likeminded countries to invest in their export enforcement capacity.** Unlike other geopolitical challenges, export enforcement cannot be effective unless there is a coordinated global effort. Without such an effort, bad actors can simply bypass one country's controls and source a sensitive commodity elsewhere.

**We've done this before.** Up until 1977, when the United States passed the Foreign Corrupt Practices Act (FCPA), no country in the world considered the bribing of foreign officials for business purposes to be illegal. Twenty years later, the Organization for Economic Cooperation and Development's (OECD) Anti-Bribery Convention was signed. **We're now beginning to see that same shift with respect to export enforcement.** Like bribing a foreign official, exporting the most sensitive goods and technologies without appropriate safeguards is a collective harm; and we must work collectively as partners — through coordinated and aggressive enforcement action — to prevent these sensitive goods and technologies from falling into the wrong hands.

But it's not enough just to impose multilateral controls; **to be effective, controls need to be aggressively enforced,** not only by the United States but through coordinated work with coalition partners. For the United States and Canada, that means coordinated work by our respective enforcement teams – my Export Enforcement team at the Bureau of Industry of Security (BIS) and Canada Border Services Agency (CBSA) here in Canada.

**This partnership is already bearing fruit.** During one of the temporary deployments last year, BIS and CBSA's Counter Proliferation Operations

Section (CPOS), working with U.S. Customs and Border Protection, stopped a shipment of drone antennas on the tarmac in Alaska before they could be illegally exported

**Collaboration on enforcement doesn't stop with just us and Canada.** We are also working to coordinate more broadly with our other Five Eyes partners, as well as with ASEAN countries like Singapore, Malaysia, and the Philippines. And just last month, the U.S.-EU Trade and Technology Council (TTC) reaffirmed the importance of enforcing export controls in a parallel manner.

**While 2022 required intense work on Russia, Russia was not our only priority.** We remain laser- focused on the risk posed by other nation-states, such as the People's Republic of China (PRC), Iran, and North Korea.

To give a recent example of the challenges we face, just two weeks ago, a California man pled guilty for violating export control laws by secretly funneling sensitive aeronautics software to a Beijing university

The recipient, Beihang University, had previously been placed on our Entity List for helping to develop the PRC's military rocket systems and unmanned air vehicle systems.

**This case helps illustrate how the domains of national security and of academia are growing increasingly interconnected.** To address this dynamic, we are actively engaging with U.S. academic institutions and research centers, in part through our Academic Outreach Initiative, on ways they can help safeguard their advanced research. We're also working closely with our Canadian counterparts in helping academic institutions protect themselves from current and future threat actors.

**We also changed our policy on how we respond to a host government that is preventing our ability to conduct end-use checks overseas...** Under our new policy, such governments now have a choice. If they cooperate and the end-use checks are successful, then companies will be removed from our Unverified List. On the other hand, if they continue to prevent our end-use checks, we will initiate the process to have companies added to our Entity List.

**After the policy became effective, we were able to complete successful end-use checks in China for the first time in over two years.** In December, we removed 25 Chinese entities from our Unverified List after the satisfactory completion of end-use checks and verification of those entities' bona fides in cooperation. **And the policy has had an impact in other ways as well.** We didn't only remove entities from our Unverified List in December – we also moved nine Russian companies onto the Entity List because of Russia's sustained failure to schedule our end-use checks.

Right now, we have ECO positions located in seven places around the world, in Beijing, Hong Kong, Frankfurt, Singapore, Istanbul, New Delhi, and Dubai. **I'm excited to share that we're now adding two more ECO positions, one in Helsinki and the other in Taiwan.** These new positions, plus our new Export Control Analyst position in Ottawa and our enhanced partnership arrangement with CBSA, mean that we now have more resources devoted to protecting U.S. and Canadian technology from diversion than ever before."

## Kendler Calls for Cooperation

In a speech marking the opening of the 2022 Massachusetts Export Expo, Assistant Secretary of Commerce for Export Administration Thea Kendler shared her experience at the Justice Department and how it informs her role enforcing Export Controls.

"Right now, we face new challenges to our security and prosperity. We are seeing national security, foreign policy, and economics intertwine like never before. Authoritarian regimes and non-state bad actors seek to turn the strength that is our economic prosperity, into a weakness they can exploit.

"The list of threats and malign actors is long, and the threat environment is ever changing. We must tailor export controls to ensure that we don't disincentivize your technological leadership and that we return resources to the United States for further innovation and research. **We must make our export controls a multilateral – or plurilateral or bilateral – system as much as possible.**

*We are seeing national security, foreign policy, and economics intertwine like never before.*

**Thea Kendler,** Assistant Secretary of Commerce for Export Administration

# On Sanctions Bus or In the Dust — Treasury's Adeyemo

**COUNTRIES AND FIRMS** that wish to trade with the US and EU will have to comply with sanctions regimes, including expanded dual-use restrictions on Russia, according to **Deputy Treasury Secretary Wally Adeyemo**.

In a presentation at the Council for Foreign Relations Tuesday, the number two treasury official discussed allied measures, their impact, and previewed further actions to expect. [edited for brevity]

"The first prong of our economic strategy is to deny the Kremlin's ability to use the money they have to buy the weapons they need. And the second is to reduce the revenues that President Putin can use to fund his war of choice and prop up the Russian economy. Put simply, we're making the Kremlin choice between funding its illegitimate war and propping up its economy harder each day. The Kremlin's choice to spend the country savings can hide the damage for now, but our actions are forcing Russia to mortgage its economic future to save face today.

"Looking to China is not a solution for Russia's challenges. While we are concerned about Russia's deepening ties with China, Beijing cannot give the Kremlin what it does not have, because China does not produce advanced semiconductors Russia needs, and nearly 40% of the less advanced microchips Russia's receiving from China are defective.

"Going forward, the breadth of this coalition is what will enable us to continue to isolate Russia. We will force those that fail to implement our sanctions and export controls to choose between their economic ties with a coalition of countries that represent 50% of GDP, or providing material support to Russia, an economy that is becoming more isolated every day. One year into the conflict, Russia's economy looks more like Iran and Venezuela's than a member of the G20.

*The first prong of our economic strategy is to deny the Kremlin's ability to use the money they have to buy the weapons they need.*

**Wally Adeyemo,** Deputy Secretary of the Treasury

## Enforcement Focus

"In addition, we and our allies are planning to launch a renewed effort to rigorously enforce the sanctions and export controls we've already put in place. Our approach to countering evasion will focus on three elements.

The first, consistent with our overall approach, will be to work closely with our allies and partners, especially in the G7 and EU. We will use sanctions, export controls and other tools to prevent the Kremlin from using the money they have to purchase the weapons and goods they need to fight this war of choice.

The second element of this effort is to identify and shut down the specific channels through which. Russia attempts to equip and fund its military. Our counter evasion efforts will deny Russia access to the dual use goods being used for the war and cut off these repurposed manufacturing facilities from the inputs they need to fill Russia's production gaps.

"The final element of our approach will be to put pressure on companies in jurisdictions we know are allowing or facilitating evasion. We have seen troubling patterns in several countries, including several Russian neighbors, where the Kremlin has deepened its financial ties and trade flows. As other markets have been closed off, we are providing intelligence and actionable information to enable countries to stamp out sanctions evasion in these jurisdictions.

"Officials from the US and the governments of our coalition partners are also engaging with companies and banks in these jurisdictions to tell them directly that if they choose to not enforce our sanctions and export controls, we will cut them off from access to our markets and financial systems.

## Call to Choose

"Fundamentally, we are all parts of the global economy and that is part of the rules

based order that was created after World War Two. Russia has violated the sovereignty of another country and therefore they should not be able to reap the benefits of being part of the international system.

"In my conversations with foreign countries, when I go to talk to them about their plans to continue to participate in buying arms from Russia, they all are skeptical because they both don't think the Russia can produce enough arms, and they've also seen how Russian arms have performed on the battlefield.

"And our message to those countries that are not already sanctioned by the international community, countries that may be playing a role in transhipment, is a simple one. Do you think that your country's economic interest are better furthered by having a relationship with Russia, economy that is relatively small in comparison to the economies of our coalition? Because fundamentally the choice we're going to give you is that you can provide material support to Russia or you can continue to do business with our economies. You can't continue to do both and that's a choice that we think companies in these countries are going to see as an easy one.

"Ultimately this is not about the United States and China. It is really about the coalition and our interest in making sure that Russia's invasion of Ukraine ends, and fundamentally for China, for the companies in China, for the individuals in China. The economic relationship with the EU, the United States, with Japan is more important than the economic relationship with Russia.

"Fundamentally, we think that like any other jurisdiction. China has to make choices about what they are willing to do and whether they want to be part of the global system that represents 50% of the global economy, or whether they want to strengthen their ties with Russia. Ultimately, the key to the system holding together is that the benefits outweigh the detractions.

## Industry Collaboration Drove Oil Price Cap

While traditionally we've had sanctions worked through banks and financial, the financial industry, this is the first time we've implemented anything like this. The most important thing we did in developing the price cap was our engagement with industry, both to help them understand what we're trying to accomplish, and for them to help us understand how best to do it.

**"We will use sanctions, export controls and other tools to prevent the Kremlin from using the money they have to purchase the weapons and goods they need to fight this war of choice," says Deputy Treasury Secretary Wally Adeyemo.**

The most important lesson from this is that, as we rely more on the private sector, a key part for us is going to be the ongoing dialogue we have with them in terms of how best to design our tools in a way that makes it easy for them to participate. Helping us to enforce them.

## Sanctions Preparations

Secretary Yellen asked me to undertake [a Sanctions Review] when I came into office. I talked to people like my foreign counterparts about what worked and what hadn't worked. Fundamentally, that review ended in the fall of 2021. Two months later, as we started to see the intelligence above about Ukraine, Russia building up troops at the border of Ukraine, I went back to those same counterparts and said we need to start planning for this contingency. And we took what we learned from that review and applied it here.

And one of the most important lessons was that the best way to protect against not only the overuse but not using them in a targeted way was to do it in a multilateral fashion. That's why we work so quick closely with our allies and partners. I think one of the most important things that we've learned from Russia's invasion

**Continues on next page**

**Continued from previous page**

of Ukraine is a lesson that we have known since World War Two, which is that one of the key strengths of the United States is the fact that we have a deep history of working closely with our allies and partners to accomplish not just our national security objectives, but our economic objectives as well.

**I'm not gonna preview any sanctions today**, but as the president said, we plan to announce additional sanctions that will look to meet our two objectives, which are to go after the military industrialized complex that Russia has and also to cut off their sources of revenue going forward.

**A big piece of what we're going to do using sanctions is also go after the networks that are helping to facilitate evasion.** So in the coming days, you'll see additional actions that we'll take not just here in the U.S., but to my larger point, in collaboration and coordination with our allies and partners around the world who are part of this coalition

My expectation is that the European Union, the United States, the rest of the G7 will act together to hold accountable any country, any company, any individual that provides material support to Russia going forward. We've already used and the tools we would use are the same tools we would use in any jurisdiction, which includes sanctions, which we've already demonstrating a willingness to use, but also furthering our export controls.

What we're going to do is further tighten our export controls and sanctions to go after some of these dual use goods that we know are furthering their war effort. It's not only an action we're going to take here in the United States. We know that the European Union is committed to taking alongside us.

For any jurisdiction, being China, be it the UAE, be it a country that is neighboring Russia, the choice they're going to have to make is not only with regard to their economic relationship with the US, but their economic relationship with the other members of our coalition, who also feel strongly about the fact that the most important thing that we can do is help Ukraine end this war as quickly as possible.

# Joint Compliance Note on Third Party Actors

**SIGNALING A REDOUBLED FOCUS** on countries providing conduits to evade western sanctions, Bureau of Industry and Security (BIS), the Department of Justice (DOJ), and Treasury's Office of Foreign Assets Control (OFAC), issued a Tri-Seal Compliance Note to alert public to how traders use third-party intermediaries and transshipment points to circumvent restrictions and obscure the true identities of sanctioned end users.

The Document called out for scrutiny of transactions routed through jurisdictions close to Russia, including China, Armenia, Turkey, and Uzbekistan. Elizabeth Rosenberg, the assistant Treasury secretary for terrorist financing and financial crimes, said on Thursday that the UAE was a "country of focus" for the U.S.

**The Note also describes common red flags** that can indicate a third-party intermediary may be engaged in efforts to evade sanctions or export controls. "Effective compliance programs employ a risk-based compliance programs that entities can adopt to minimize the risk of evasion. These compliance programs should include management commitment (including through appropriate compensation incentives), risk assessment, internal controls, testing, auditing, and training. "These efforts empower staff to identify and report potential violations of U.S. sanctions and export controls to compliance personnel such that companies can make timely voluntary disclosures to the U.S. government. Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

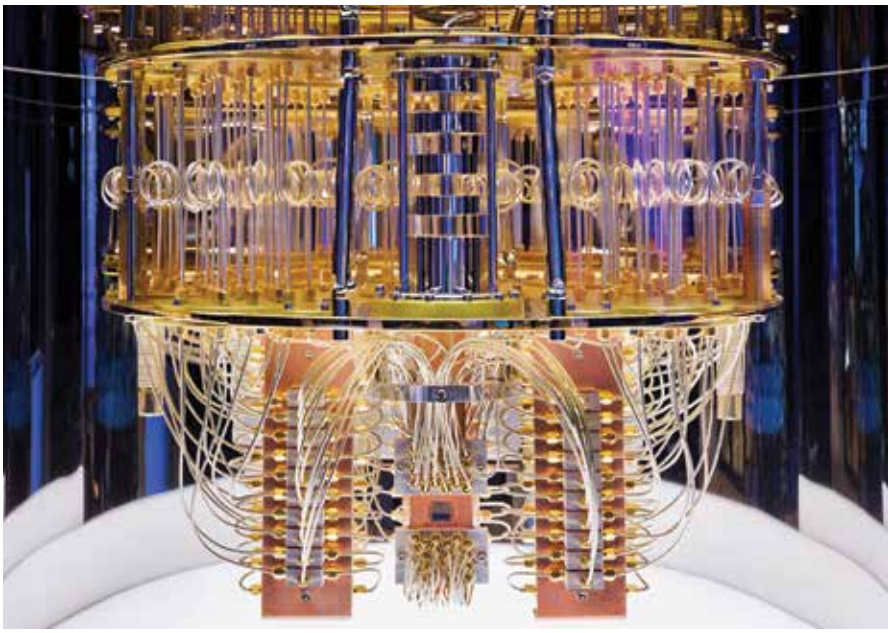
## Red Flags

Common red flags can indicate that a third-party intermediary may be engaged in efforts to evade sanctions or export controls, including the following:

- Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions;
- A customer's reluctance to share information about the end use of a product, including reluctance to complete an end-user form;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Declining customary installation, training, or maintenance of the purchased item(s); IP addresses that do not correspond to a customer's reported location data;
- Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
- Payment coming from a third-party country or business not listed on the End-User Statement or other applicable end-user form;
- Use of personal email accounts instead of company email addresses;
- Operation of complex and/or international businesses using residential addresses or addresses common to multiple closely-held corporate entities;
- Changes to standard letters of engagement that obscure the ultimate customer;
- Transactions involving a change in shipments or payments that were previously scheduled for Russia or Belarus;
- Transactions involving entities with little or no web presence; or
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to Russia or Belarus. Such locations may include China (including Hong Kong and Macau) and jurisdictions close to Russia, including Armenia, Turkey, and Uzbekistan.

## Best Practices

Best practices in the face of such risks can include screening current and new customers, intermediaries, and counterparties through the Consolidated Screening List and OFAC Sanctions Lists, as well as conducting risk-based due diligence on customers, intermediaries, and counterparties. Companies should also regularly consult guidance and advisories from Treasury and Commerce to inform and strengthen their compliance programs.



**Interior of an IBM Quantum computing system. Sensitive items at issue included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic, and nuclear weapons development.**

IBM

## Follow Enforcement Actions

Companies should also review BIS and OFAC enforcement and targeting actions, as they often reflect certain tactics and methods used by intermediaries engaged in Russia-related sanctions and export evasion. OFAC's civil enforcement actions also illustrate a range of sanctions evasion techniques employed across multiple sanctions programs, including falsifying transactional documents, omitting information from internal correspondence, and shipping goods through third countries. DOJ has pursued criminal charges against those who it alleges are using front companies and intermediate transshipment points to evade Russia-related U.S. sanctions and export controls. In many cases, DOJ finds that the defendants use shell companies and transshipment points in third-party countries to evade sanctions and procure powerful dual-use items for use by the Russian defense sector 15. The sensitive items at issue included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic,

**Continues on next page**

**Continued from previous page**

and nuclear weapons development as well as advanced semiconductors and microprocessors used in fighter aircraft, missile systems, smart munitions, radar, and satellites. In one of the cases, the indictment alleges that U.S.-manufactured component parts were found in seized Russian weapons platforms in Ukraine.

## Tactics To Evade Detection Have Included The Following:

- Claiming that shell companies located in third countries were intermediaries or end users; in one case, DOJ alleges that only one of the five intermediary parties had any visible signage and consisted of an empty room in a strip mall;
- Claiming that certain items would be used by entities engaged in activities subject to less stringent oversight; on at least one occasion, a defendant allegedly claimed that an item would be used by Russian space program entities, when in fact the item was suitable for military aircraft or missile systems only;
- Dividing shipments of controlled items into multiple, smaller shipments to try to avoid law enforcement detection;
- Using aliases for the identities of the intermediaries and end users;
- Transferring funds from shell companies in foreign jurisdictions into U.S. bank accounts and quickly forwarding or distributing funds to obfuscate the audit trail or the foreign source of the money;
- Making false or misleading statements on shipping forms, including underestimating the purchase price of merchandise by more than five times the actual amount;
- Claiming to do business not on behalf of a restricted end user but rather on behalf of a U.S.-based shell company.
- Businesses of all stripes should act responsibly by implementing rigorous compliance controls, or they or their business partners risk being the targets of regulatory action, administrative enforcement action, or criminal investigation

NAVY.MIL

**The Navy and Army demonstrate advanced hypersonic technologies.**

## Voluntary Self Disclosure Encouraged

Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Information about **BIS's Voluntary Self-Disclosure ("VSD") Policy** can be found in Part 764.5 of the Export Administration Regulations or in the enforcement section of BIS's website www.bis.doc.gov.

**OFAC's Enforcement Guidelines,** which provide incentives for voluntary self-disclosure, are available at 31 CFR Part 501, Appendix A as well as in OFAC Frequently Asked Questions: https://home.treasury.gov/policy-issues/financial-sanctions/faqs/13. All potentially criminal violations of sanctions and export control laws should be disclosed to the Department of Justice's National Security Division, Counterintelligence and Export Control Section. More information about DOJ's VSD Policy is available at https://www.justice.gov/nsd/export-control.

These principles apply broadly to all U.S. government enforcement regimes, including the **Disruptive Technology Strike Force**, which was announced on February 16, 2023. That Strike Force, co-chaired by DOJ and Commerce, focuses on investigating and prosecuting the illicit transfer of sensitive technologies to hostile nation states.

# McCaul Leans In on BIS Coddling Chinese

**HOUSE FOREIGN AFFAIRS COMMITTEE Chairman Michael McCaul** released his interpretation of data on licensing outcomes from the Department of Commerce's Bureau of Industry and Security (BIS) following a heated grilling of BIS Chief Alan Estevez by the full committee earlier in the week.

In a one page handout released by his office, the ten-term Texan showed that in a three month period last year, Commerce approved 192 Licenses representing $23 billion in goods to sanctioned Chinese firms.

"It is unacceptable BIS approved more than $23 billion worth of licenses to sell U.S. technology to blacklisted companies based in China. This critical U.S. technology is going to the Chinese Communist Party's surveillance and military efforts. BIS must and can do more."

The Biden administration has been considering limiting the items it authorizes U.S. companies to ship to telecoms equipment giant Huawei Technologies Co, which was added to a blacklist in 2019 but which continues to receive billions in U.S. goods under a special plan implemented by the Trump administration.

Responding to McCaul's complaints during the Committee hearing, **BIS Chief Alan Estevez** clarified the state of play.

"We have specific licensing rules; the entity list is not a blanket embargo. So going on the entity list may have a particular rule… The licensing rule of the previous administration that still stands for Huawei allows things below 5G, below cloud level to go," said Mr. Estevez. "I will say that all those things are under review."

Mr. Estevez added that the administrations October 2022 restrictions on chipmaking equipment had already made ineligible many of the previously licensed sales.

---

# Belt & Road Courts (CICC) Report Released

**THE U.S.-CHINA COMMISSION** released a new staff research report on China's International Commercial Court (CICC). The report explores the "one-stop shop" dispute resolution center for Belt and Road Initiative (BRI)-related commercial disputes.

## Highlights

The China International Commercial Court's (CICC) establishment in 2018 is part of a broader push by the Chinese Communist Party (CCP) to reshape international norms in its favor. While the CCP cites the CICC as a new step in the evolution of China's legal system, the court's basic structure and the fact that it is directly under CCP control mean that foreign parties, including U.S. parties, are at risk of biased judgments.

China's government has cited the CICC as evidence of the country's increasing openness. In many respects, however, the CICC prevents effective foreign participation, including by preventing foreign lawyers from participating in proceedings. The unusually restrictive nature of the CICC compared with other international dispute resolution forums has raised concerns that the CICC will be biased in favor of Chinese parties.

While the CICC has only adjudicated a handful of cases so far, the court represents another avenue for the CCP to advance its discourse power, allowing for the promotion of Chinese legal venues and approaches alongside Chinese-funded projects abroad. This could allow the CCP to legitimize its dual foreign dispute system, promoting international enforcement of Chinese judgments while reserving the power to disregard foreign judgments when the CCP deems them to be against its interests.

The limited international enforceability

**Continues on next page**

CFIUS

## Five Eyes Exceptions

➤ Based on their establishment and use of their own robust foreign investment screening programs, the Committee on Foreign Investment in the US (CFIUS) has determined that New Zealand and the United Kingdom have met the Excepted Foreign States (EFS) determination requirements under CFIUS regulations.

This ensures those countries' continued status as excepted foreign states pursuant to CFIUS regulations and the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), absent further action from CFIUS.

With this action qualifying investors from all Five Eyes countries will now continue to benefit from exception from CFIUS jurisdiction over certain noncontrolling transactions, real estate transactions, and mandatory filing requirements as established under law.

"Today's actions reflect that our Five Eye allies have all stood up and implemented their own robust foreign investment screening programs. We look forward to continuing to coordinate with all of them on matters relating to investment security," noted **Assistant Secretary for Investment Security Paul Rosen**

These actions reflect continued effort by partners across the Five Eyes Alliance to establish and operate effective and robust investment screening authorities to address national security risk that can arise from foreign investment while maintaining open investment.

**The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the UK and the U.S.** These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence. The "Five Eyes" term has its origins as a shorthand for a "AUS/CAN/NZ/UK/US EYES ONLY".

**Continued from previous page**

of CICC judgments presents a key challenge for the CICC, since foreign commercial parties may be reluctant to choose a court where the recognition and enforcement of judgments are not guaranteed.

The international enforceability of arbitration awards from CICC-approved institutions is far-reaching. China is a contracting state to the New York Arbitration Convention on the Recognition and Enforcement of Foreign Arbitral Awards, so CICC arbitration awards can be enforced in the more than 170 countries that are contracting states.

FISA

## Section 702 Re Approval Campaign Kickoff

**MARKING THE KICKOFF** of a campaign to build support for the extension of Section 702 of the Foreign Intelligence Surveillance Act (FISA), Assistant Attorney General Matthew Olsen defended the measure in a speech at the Brookings Institution Feb. 28, 2023.

The Chief of the Justice Department's National Security Division praised the utility of the Act's "warrantless surveillance," and gave assurances that lessons lad been learned. The post 9/11 surveillance law permits government collection of communications of foreigners abroad, to include their interactions with Americans, without obtaining a warrant.

This suspension of Citizens' Fourth Amendment protections has prompted concerns from civil rights and privacy advocates, while elements of the political right piled on. House Judiciary Committee Chair Jim Jordan (R-OH) and House Intelligence Committee Chair Mike Turner (R-OH) have both opposed the Act as it stands, with Mr. Jordan calling for its sunset and Mr. Turner naming a GOP working group to guide the reforms.

### Excerpts from Olson's Speech

"What keeps me up at night is thinking about what will happen if we fail to renew Section 702 of FISA. This law will expire on December 31st of this year if Congress doesn't act to reauthorize it. If 702 expires or is watered down, the United States will lose critical insights we need to protect the country.

"Section 702 enables the United States government to gain intelligence about our most pressing threats. Today, we are relentlessly focused on serious threats, such as:

- The Chinese government's efforts to spy on us and steal our technology;
- Iran's sanctions evasions;
- North Korea's nuclear program; and
- Russia's invasion of Ukraine.

"The bottom line is that Section 702 gives us the intelligence necessary to stay one step ahead of our adversaries. We cannot afford to allow it to lapse. And it is too important to the interests of the U.S. and our allies — and to our basic safety — to wait for the 11th hour to do so.

"When I first came to NSD in 2008, I was part of the team that helped craft Section 702. I went on to become the General Counsel at NSA where I oversaw NSA's implementation of 702 and saw, in practice, both the power of 702 as a collection tool and the rigor of the oversight procedures that are built into it.

"When FISA was originally passed, Congress intended for the law to regulate surveillance activities conducted within the United States. But with the advent of the internet, and as the technology supporting international communications evolved, FISA's terms required the government to seek individualized court orders, even when the target of the collection was a foreign person based overseas.

"Unfortunately, in this highly sensitive area, we've made mistakes in recent years that have undermined trust…. We've implemented key reforms But I want to be clear, this is about more than just imposing a checklist of new requirements… we are building a culture of compliance."

# Honeywell Dealer Indicted for Avionics Exports

**JUSTICE ANNOUNCED THE ARREST** of the principals of a Kansas avionics distributor for the export of aviation technology from the United States to Russia and Russian end users located in other countries.

Cyril Buyanovsky and Douglas Robertson owned and operated the transparently named KanRus Trading Company, authorized distributors of BendixKing aircraft control instruments.

Since 2020, the defendants conspired to evade U.S. export laws by concealing and misstating the true end users, value and end destinations of their exports and by transshipping items through third-party countries.

Transshipment points included Germany, the UAE, Cyprus, Laos and Armenia to conceal the true end users and end destinations; funds for the sales flowed from. bank accounts in the UAE, Russia, Cyprus, and Armenia to KanRus's bank account in the United States

In once instance, a KanRus customer shipped collision avoidance equipment (TCAS) components from South Sudan to the UAE to KanRus in Kansas. The reported U.S. customs value on the shipment was $100.

One of the pieces returned for refurbishment was a TCAS computer processor with an inventory sticker from the Federal Security Service of the Russian Federation (FSB), the principal intelligence and security agency of the Russian government.

Another transaction involved an EEI that listed the value of the export as $6,118 and the ultimate consignee in Germany when, in fact, the avionics shipment was valued at $159,625 and was destined for Russia.

In February 2022, Buyanovsky ordered Honeywell BendixKing KT-74 transponders and attempted to ship them to Russia. The shipment was detained by the U.S. Government, after which BIS directly informed him that a license was required to export the KT-74 transponders to Russia. Buyanovsky then began routing his shipments to a residential address in Cyprus, with later routes including Laos and Armenia.

Two months before his arrest, Buyanovsky may have concluded that after 14 years, the juice wasn't worth the squeeze.

" I became licensed by the State of Kansas for Health and Sickness Insurance sales. So here I go, much to learn and much to help people. It's a jungle out there with health insurance, and I am hoping to add some clarity and save some

**Continues on next page**

BIS/DDTC

# Blueprint and Alloy Exports Yield Settlements

**ADDITIVE MANUFACTURER** 3D Systems agreed to pay $12,777,750, engage a consultant and complete compliance audits to settle allegations of violations of Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR) by exporting controlled aerospace technology and metal alloy powder to China without the required license, and by exporting controlled technology to

**Continues on next page**

**Continued from previous page**

Germany without the required license, as well as failing to comply with EAR and ITAR recordkeeping requirements.

"Today's enforcement action highlights a troubling trend of U.S. companies offshoring 3D printing operations and ignoring the export controls on the technical data sent overseas to facilitate the 3D printing," said **OEE Director John Sonderman**. "The enforcement action would not have been possible without a defense contractor coming forward when they noticed that a price quotation indicated that the quoted parts were to be manufactured in Asia using controlled technology.

Last June, BIS issued a Temporary Denial Order barring North Carolina based **Rapid Cut** and affiliates for similar behavior.

During the time period at issue, 3D Systems provided 3D printing, cast urethane modeling, and injection molding services to customers across the U.S. and abroad. While 3D Systems maintained its own manufacturing facilities in the U.S., it also regularly e-mailed design documents, blueprints, and technical specs to its then-subsidiary Quickparts office in China to generate a price quote for On Demand Manufacturing (ODM). The e-mails, which included controlled U.S. technology, constitute an export of technology subject to the EAR.

On several occasions, and unbeknownst to the U.S. companies that requested the price quotes, 3D Systems e-mailed controlled design drawings, including those for military electronics as well as those used in the development, production, operation, or repair of spacecraft, to its then-subsidiary's office in Guangzhou City, China. 3D Systems also exported controlled design documents to Germany, where 3D Systems maintained a mirrored server to store employee e-mails containing controlled technology.

In addition to unlicensed exports via e-mail, 3D Systems also exported metal alloy powder, which is controlled for national security and nuclear nonproliferation reasons, to China without the required BIS license.

In 2015, a Quickparts customer notified Quickparts of potential violations of the Regulations in connection with the export of technology subject to the Regulations to China. The customer also informed Quickparts that it had submitted a disclosure to the U.S. government regarding such potential violations.

Eighteen months later, in connection with the disclosure, a BIS Special Agent conducted an outreach with 3D Systems' then-Director of Operations and Special Projects. In April 2017, BIS issued a Warning Letter to 3D Systems regarding the conduct described in the disclosure.

3D Systems therefore knew or had reason to know that the technology it handled regularly as part of its ODM business unit was subject to the Regulations and likely required BIS licenses prior to its release to most countries, including China.

However, despite the outreach and explanation by a BIS Special Agent of the company's export control compliance obligations under the Regulations, 3D Systems failed to seek or obtain a license for such technology before exporting it. Other violations cited by DDTC included unauthorized reexports of technical data to Taiwan and unauthorized exports of technical data to foreign-person employees

The company has been undertaking corrective actions by expanding the scope of its internal investigation to cover exports of technical data; implementing remedial compliance measures; selling its business unit primarily responsible for ITAR activity; and signing a statute of limitations agreement tolling the statutory period. For these reasons, the Department has determined that it is not appropriate to administratively debar 3D Systems Corporation.

3D Systems spun off its On Demand Manufacturing business to the buyout group Trilantic in 2019.

---

FCPA

## Justice Buries the Hatchet with Ericsson

**SWEDISH TELECOMS GIANT** and serial FCPA violator LM Ericsson signed a new deal with the

Justice Department acknowleging further breaches of the deferred prosecution agreement it entered into for corruption in Djibouti, China, Vietnam, Indonesia and Kuwait.

According to the documents, Ericsson withheld evidence relating to the China and Djibouti cases, as well as failed to report and disclose their illicit alliance with the Islamic State in Iraq uncovered last year.

**Ericsson will enter a guilty plea regarding previously deferred charges relating to conduct prior to 2017**. The new plea agreement calls for $207 million in additional fines and extension of the independent compliance monitor until June 2024.

The announcement comes 12 months after the disclosure that Justice intended to find it in violation of its 2019 Deferred Prosecution Agreement (DPA) after the International Consortium of Investigative Journalists published "The Ericsson List," documenting the firm's extensive dealings with the terrorist group Islamic State in Iraq between 2011 and 2019.

In 2013 Ericsson disclosed that it was cooperating with U.S. authorities investigating bribery allegations, resulting in a $1 billion settlement in 2019. That settlement contained no mention of Iraq.

**Shareholders voted last March to hold CEO Börje Ekholm and the Board personally liable for the scandal.** "This resolution is a stark reminder of the historical misconduct that led to the DPA. We have learned from that and we are on an important journey to transform our culture," Ekholm said in a statement announcing the settlement.

FCPA

## Petrobras "Car Wash" Indictments

➤ A Connecticut man and a foreign national have been charged with conspiracy, multiple counts of violating the Foreign Corrupt Practices Act (FCPA), and money laundering in connection with an alleged scheme to pay bribes to Brazilian officials to win contracts with Brazil's state-owned and state-controlled energy company, Petróleo Brasileiro S.A. – Petrobras (Petrobras). The indictments are part of a larger investigation by Brazilian authorities known as Operation Car Wash begun in 2014. **Glenn Oztemel** (64) and **Eduardo Innecco** (73), employed by Freepoint Commodities, LLC are alleged to have paid consulting fees and commissions to Innecco, knowing that Innecco would pay a portion of those funds to Brazilian officials as bribes.

Oztemel and Innecco are each charged with conspiracy to violate the FCPA, conspiracy to commit money laundering, three counts of violating the FCPA, and two counts of money laundering. They face up to five years in prison for each of the bribery conspiracy and bribery charges, and up to 20 years in prison for each of the money laundering conspiracy and money laundering charges.

## Russian Charged in Procurement Scheme

➤ **Ilya Balakaev**, 47, of Moscow, was charged in the Eastern District of New York with offenses related to a years-long scheme to illegally smuggle sensitive devices used in counterintelligence operations from the U.S. to Russia for the benefit of the Federal Security Service of the Russian Federation (FSB), the principal intelligence and security agency of the Russian government.

Balakaev is further charged with illegally exporting a gas detector and related software from the United States to Russia for the benefit of North Korea (DPRK).

Balakaev would purchase the electronic devices on the internet or directly through the United States-based manufacturers and ship them to an accomplice's home in Richmond, Va. Then Balakaev flew to the U.S. to pick up the devices and bring them back to Russia or had others ship the electronic devices to Russia.

**The electronic devices Balakaev purchased, repaired, and sold to the FSB and DPRK are subject to the EAR** and included spectrum analyzers and signal generators.

**Balakaev was aware of the applicable U.S. export control laws** which prohibited him from purchasing the electronic devices in the U.S. for ultimate use by the FSB and DPRK. As described in the indictment, on or about Nov. 5, 2019, his Richmond colleague emailed Balakaev a hyperlink to a BIS document titled "Don't Let This Happen To You!: Actual Investigations of Export Control and Antiboycott Violations." In the email, he told Balakaev to "Take a look just in case."

The BIS document provided "an introduction to the consequences of violating U.S. export control law." In addition to explaining U.S. export control laws, the document noted specific examples of individuals who violated U.S. sanction regulations by exporting items to Russia without a BIS license. Balakaev subsequently downloaded the document and saved the document to his computer.

Concurrently, Commerce Department separately issued a Temporary Denial Order denying the export privileges of Balakaev and his company, Radiotester OOO, for 180 days with the possibility of renewal.

**Skyline of Dubai, United Arab Emirates**

PEXELS: TIMO VOLZ

# Treasury Calls Out UAE for Sanctions Busting

**Elizabeth Rosenberg, the assistant Treasury secretary for terrorist financing and financial crimes,** added to the drumbeat of criticism of sanction dodging regimes, telling a meeting of Women in International Trade that the UAE was a "country of focus" for the US.

"Our sanctions have played an important part in this very broad effort. From the beginning, they have been designed to constrain the wealth and weapons available to Putin to fight his war—and to do so in a way that minimizes the harm to our own economy.

"But Russia will look for ways to work around our measures. **The coming year will be about ensuring that our sanctions architecture is fully enforced and effective—in particular, by figuring out and cracking down on the ways Russia evades sanctions**. Furthermore, we will deploy new and novel ways of complementing trade controls with financial constraints to shut down the evasion and shadowy economic activity Russia seeks to sustain its war efforts.

"We are specifically concerned about increases in trade with Russia in the kind of goods that can be used on the battlefield and those who are aiding designated Russian entities. We are investigating this type of assistance at the individual, firm, and sector level. We will engage companies, banks, regulators, and service providers in a series of jurisdictions we assess are wittingly or unwittingly providing assistance to Russia. This is a broad campaign on which we are working closely with allies and partners.

"To give you an example from one country of focus for us: we are concerned that between July and November of 2022 United Arab Emirates (UAE) companies exported over $18 million worth of goods to U.S.-designated Russian entities.

"Also, between June and November of 2022, UAE companies exported over $5 million worth of U.S.-origin, U.S.-export controlled goods to Russia, including but not limited to semiconductor devices, some of which can be

used on the battlefield.

"This is about making the choice clear to companies and banks: you can do business with the countries that constitute more than 50 percent of the world's GDP, and its most convertible and stable currencies, or do business with those who facilitate Russia's war."

*"We are specifically concerned about increases in trade with Russia in the kind of goods that can be used on the battlefield and those who are aiding designated Russian entities."*

**Elizabeth Rosenberg,** Assistant Secretary for Terrorist Financing and Financial Crimes

# White House Amps Up Pressure on Russia

**THE WHITE HOUSE MARKED** the anniversary of Russia's invasion of Ukraine with a raft of spending, tariffs, sanctions and export controls aimed at Russia and her enablers.

## Tariffs on Steel, Aluminum & Chemicals

President Biden raised tariffs on most metal and metal products – doubling them from 35 to 70 percent. Further tariffs were increased on additional Russian products to 35 percent, including chemicals and minerals.

The actions increased tariffs on Russian aluminum pursuant to Section 232 of the Trade Expansion Act of 1962, as amended. Along with the second round of tariff increases on certain Russian products under the Suspending Normal Trade Relations with Russia and Belarus Act **these actions will increase tariffs on Russian aluminum up to 270 percent**, according to a statement from Commerce Secretary Raimondo.

## Funding Increased

Additional funding announced Friday included **$9.9 billion in grants for healthcare, education, and emergency services.** This budget support is being disbursed via the World Bank's Public Expenditures for Administrative Capacity Endurance (PEACE) mechanism on a reimbursement basis once expenses have been verified.

The Department of Energy continues its support for the country's electrical grid with additional shipments of switchgear, transmission and generation equipment, and $250 million in additional emergency energy assistance "to help Ukraine further strengthen its grid."

Along with the Ukrainian aid, the White House announced $300 million in emergency energy assistance for Moldova, working to increase local electric power generation, provide fiscal support, and improve interconnectivity between Moldova and the European Union.

## FDP/EAR99 Export Controls Expanded

The Commerce Department announced two new rules, one to broaden the industry reach of earlier sanctions, as well as measures to address directly Russian use of Iranian unmanned aerial vehicles (UAVs) in the conflict.

**"Export Control Measures on Iran Under the Export Administration Regulations (EAR) to Address Iranian Unmanned Aerial Vehicles (UAV) and Their Use by Russia Against Ukraine"**

Imposes new export control measures on Iran in order to address the use of Iranian UAVs by Russia in its ongoing war against Ukraine by:

- **Imposing license requirements for a subset of generally low-technology ("EAR99") items**, including semiconductors that are destined for Iran, regardless of whether a U.S. person is involved in the transaction.
- **Establishes a new list (Supplement No. 7 to part 746)** identifying these EAR99 items by HTS-6 Code to allow BIS and other U.S. government agencies to track and quantify these exports.
- **Creates a new "Iran Foreign Direct Product (FDP) Rule"** specific to Iran for items in certain categories of the Commerce Control List and EAR99 items identified in the new supplement.
- **Revises the existing Russia/Belarus FDP rule to cover EAR99 items** that have been found in UAVs contain parts and components branded U.S. or U.S.-origin (although they may not actually be U.S. branded or U.S.-origin) which will help to

**Continues on next page**

**Continued from previous page**

ensure that U.S. products are not available for shipment to Iran for use in the manufacture of UAVs being used by Russia in Ukraine.

These controls are in addition to BIS's action on January 31, 2023, which added seven Iranian entities involved in the manufacture of UAVs to the Entity List as Russian 'Military End Users,' thereby subjecting them to some of the most comprehensive export restrictions under the EAR, including on foreign-produced items under the Russia/Belarus Military End User FDP rule.

**"Implementation of Additional Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR) and Refinements to Existing Controls"**

Revises the EAR to enhance the existing sanctions against Russia and Belarus by expanding the scope of the Russian and Belarusian industry sector restrictions (oil and gas production; commercial and industrial items; chemical and biological precursors) and the 'luxury goods' sanctions to better align them with the controls that have been implemented by U.S. allies and partners imposing substantially similar controls on Russia and Belarus. This rule also refines other existing controls on Russia and Belarus that were imposed in response to the February 2022 invasion.

### Entity List Expanded

Commerce is adding 86 entities under 89 entries (due to some entities operating in multiple countries) to the Entity List for a variety of reasons related to their activities in support of Russia's defense-industrial sector and war effort. Seventy-nine of the entities are added under the country heading of Russia, five are listed under the country heading of China, two are based in Canada, and France, Luxembourg, and the Netherlands each have one entry. Several of the entities in these countries are subsidiaries of entities based in China and Russia. [FR 2023-04099] and [FR 2023-03929]

### OFAC Actions

Treasury's Office of Foreign Assets Control (OFAC) is issuing Russia-related

- General License 8F, "Authorizing Transactions Related to Energy,"
- General License 13D, "Authorizing Certain Administrative Transactions Prohibited by

## SANCTIONS BRIEFS

### BIS Blacklist Growth Continues

➤ The Bureau of Industry and Security added 37 entities under 38 entries to the Entity List March 2nd, including 28 Chinese firms.

Infractions included, among other activities, contributing to Russia's military and/or defense industrial base, supporting PRC military modernization, and facilitating or engaging in human rights abuses in Burma and in the People's Republic of China (PRC).

"We will continue to send the world a simple message—the United States will not allow diversion of peaceful trade in ways that undermine our values and weaken our security. That's exactly what we are saying today," said Under Secretary of Commerce for Industry and Security Alan F. Estevez.

Sanctioned entities include AIF Global Logistics, and units of Genomics firm BGI and cloud services firm Inspur. , Reuters previously reported BGI was collecting genetic data from millions of women for sweeping research on the traits of populations, and collaborates with China's military.

### G7: Establishes Enforcement Mechanism, Dodges Diamonds

➤ G7 leaders announced their intention to create a formal enforcement mechanism, and vowed to take further measures, though in a nod to Antwerp, they only promised to "work collectively on further measures on Russian diamonds, including rough and polished ones, working closely to engage key partners.

"We will maintain, fully implement and expand the economic measures we have already imposed, including by **preventing and responding to evasion and circumvention through the establishment of an Enforcement Coordination Mechanism** to bolster compliance and enforcement of our measures and deny Russia the benefits of G7 economies.

"We call on third-countries or other international actors who seek to evade or undermine our measures to cease providing material support to Russia's war, or face severe costs. To deter this activity around the world, we are taking actions against third-country actors materially supporting Russia's war in Ukraine. We also commit to further aligning measures, such as transit or services bans, including to prevent Russian circumvention.

"We will adopt further measures to prevent Russia from accessing inputs that support its military and manufacturing sectors, including, among others, industrial machinery, tools, construction equipment, and other technology Russia is exploiting to rebuild its war machine."

Noting than "Russia bears full responsibility for the war and the damage it has caused, including to Ukraine's critical infrastructure" the leaders vowed to continue to freeze

Directive 4 under Executive Order 14024,"
• General License 60, "Authorizing the Wind Down and Rejection of Transactions Involving Certain Entities Blocked on February 24, 2023,"
• and General License 61, "Authorizing Transactions Related to Debt or Equity of, or Derivative Contracts Involving, Certain Entities Blocked on February 24, 2023."
• Additionally, OFAC is issuing five associated Frequently Asked Questions (1114-1118).
• OFAC is also publishing a Determination Pursuant to Section 1(a)(i) of Executive Order 14024.
• OFAC is also imposing sanctions on 22 individuals and 83 entities

While Russian banks representing over 80 percent of total Russian banking sector assets are already subject to U.S and international sanctions, OFAC today is designating over a dozen financial institutions in Russia, including one of the top-ten largest banks by asset value.

OFAC is enhancing and expanding its use of Russia-related sanctions authorities by issuing a determination that **identifies the metals and mining sector** of the Russian Federation economy pursuant to section 1(a)(i) of Executive Order (E.O.) 14024. This action complements existing provisions for sanctions against those that operate or have operated in the quantum computing, accounting, trust and corporate formation, management consulting, aerospace, marine, electronics, financial services, technology, and defense and related materiel sectors of the Russian Federation economy.

Entities named include firms that produce or import specialized, high-technology equipment used by Russian defense entities and companies that make advanced materials used in Russian weapons systems, notably carbon-fiber materials.

Individuals named included Swiss-Italian businessman Walter Moretti and several German and Swiss associates alleged to have covertly procured sensitive Western technologies and equipment for Russian intelligence services and the Russian military, including hydraulic presses, armament packages, and armor plating. Moretti and his associates have also procured equipment for Russia's nuclear weapons laboratories.

---

sovereign assets until a resolution is reached.

## China Blacklists U.S. Defense Contractors

➤ China touted its own sanctions blacklist, placing Lockheed Martin and Raytheon Missiles & Defence to China's "Unreliable Entity List" over their participation in arms sales to Taiwan.

**"Unreliable Entities"** are:
• prohibited from engaging in import and export activities related to China;
• prohibited from making new investments in China; and
• subject to fines of twice the contract value of their arms sales to Taiwan since September 2020, when the list was established. Further fines will be imposed if payment is not made within 15 days.

The use of the measure "is strictly limited and aimed at very few foreign entities breaking the law," according to the Ministry of Commerce. In February 2022, Lockheed and Raytheon were targeted by China over a missile defense system the two firms agreed to provide to Taiwan. Raytheon units Pratt & Whitney and Collins Aerospace remain unaffected by the move.

**Missing from the announcement was Boeing, Taipei's supplier of Harpoon anti-ship missiles.** Last September, China levied sanctions against Boeing Defense, Space & Security chief executive Ted Colbert and Raytheon chief executive Gregory Hayes in retaliation for those missile sales.

## KleptoCapture Grabs Metals Baron's Digs

➤ The U.S. Attorney for the Southern District of New York filed a civil forfeiture complaint against six real properties located in New York, New York; Southampton, New York; and Fisher Island, Florida, worth approximately $75 million, owned by **Viktor Vekselberg**.

The complaint alleges that the properties beneficially owned by the Ukranian-born, Russian–Israeli-Cypriot metals baron are the proceeds of sanctions violations and were involved in international money laundering transactions. The case arises in the wake of the indictment of Vekselberg's alleged strawman, **Vladimir Voronchenko**, a fugitive previously charged in the Southern District of New York.

OFAC designated Vekselberg a Specially Designated National (SDN) in 2018. Prior to his designation by OFAC, between 2008 and 2017, Vekselberg, through a series of shell companies, acquired six real properties in the U.S., today worth approximately $75 million: An eight bedroom home in Southampton, N.Y.; two units in 515 Park Avenue, New York City; and three units on Fisher Island in Miami Beach.

In April 2022, in the first seizure of an asset belonging to a sanctioned individual with close ties to the Russian regime, Justice and Spanish Authorities impounded *M/Y Tango*, a 255 foot motor yacht owned by Vekselberg. *Tango* remains moored in Mallorca.

JUSTICE & BIS

# Export Enforcement Task Force

**THE NATIONAL SECURITY DIVISION** of Justice and the Commerce's Bureau of Industry and Security (BIS) are joining with the FBI, Homeland Security Investigations (HSI) and 14 U.S. Attorneys' Offices to create a "Disruptive Technology Task Force" to enforce export controls.

"Our goal is simple but essential: to strike back against adversaries trying to siphon our best technology," said **Deputy Attorney General Lisa O. Monaco**. "Using real-time intelligence and 21st century data analytics, the Disruptive Technology Strike Force will bring together the Justice and Commerce Departments' expertise to strike back against adversaries trying to siphon off our most advanced technology, and to attack tomorrow's national security threats today."

**Monaco**

The strike force will be co-led by **Assistant Attorney General Matthew G. Olsen** of the Justice Department's National Security Division and **Assistant Secretary for Export Enforcement Matthew Axelrod** of the Commerce Department's Bureau of Industry and Security.

The initiative will focus on end users of national security concern who seek technologies related to supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences. Technologies in these fields can be used to improve calculations in weapons design and testing; improving the speed and accuracy of military or intelligence decision-making; and breaking or developing unbreakable encryption algorithms that protect sensitive communications and classified information.

"Advances in technology have the potential to alter the world's balance of power," said Assistant Secretary Axelrod. "This strike force is designed to protect U.S. national security by preventing those sensitive technologies from being used for malign purposes."

The strike force's work will focus on investigating and prosecuting criminal violations of export laws; enhancing administrative enforcement of U.S. export controls; fostering partnerships with the private sector; leveraging international partnerships to coordinate law enforcement actions and disruption strategies; utilizing advanced data analytics and all-source intelligence to develop and build investigations; conducting regular trainings for field offices; and strengthening connectivity between the strike force and the Intelligence Community.

### CFIUS in Focus

Monaco's announcement was during a speech Februrary 16th at Chatham House in London, during which she discussed Justice's work on cyber security, as well as "updating our regulatory tools to ensure we protect against foreign investments that threaten our national security."

"CFIUS began in an era of brick-and-mortar transactions. Today, the greatest risks come not from investment in our physical assets, but from transactions where datasets, software, and algorithms are the assets, Monaco said. "We are exploring how to monitor the flow of private capital in critical sectors and ensure that our own 'outbound investment' in dual-use technology doesn't provide our adversaries with a national security advantage," Monaco added.

## China to Expand Export Controls

**CHINA WILL ACCELERATE** the establishment of a modernized export control system, featuring improvements in laws and regulations, government officials said on Thursday at a forum on export control compliance, the China Daily newspaper reported.

The central government will also strengthen guidance and assistance for enterprises facing rising protectionism and abuse of export control in some countries to better protect their legitimate rights and interests, the officials said.

"The Chinese government believes that export control should follow the principles of 'fairness, impartiality and nondiscrimination', and strongly opposes abuse of export control, and unilateral sanctions and long-arm jurisdiction, which have no basis in international law," said Wang Shouwen, vice-minister of commerce and China international trade representative.

Wang said the country will coordinate development and security, as well as openness and security, "to strike a balance between export control and the promotion of law-based trade in the new circumstances." According to the vice-minister, China is making efforts to release its regulations on export control of dual-use items as soon as possible in order to enhance its legal system on the matter and provide better support to enterprises. Dual-use items are those items that can be used for both civil and military purposes.

Jiang Chenghua, head of the bureau of industrial safety and import and export control, the Ministry of Commerce, said the legislation process of the draft regulations on export control of dual-use items, which were released by the ministry in April 2022 to seek public opinion, has been accelerated, while the country's export control list is also under constant improvement.

Based on national conditions and advanced international experiences and practices, China has been constantly improving its legal and management mechanisms for export control in order to accelerate the establishment of a modern export control system with Chinese characteristics, Jiang said.

Law-based internationalized and standardized export control compliance is the historical trend, Jiang said, adding that the ministry released the guideline on internal compliance for export control of dual-use items in 2021. The guideline helps enterprises enhance their awareness and improve their ability to follow the law by establishing an internal compliance system.

Officials and experts at the forum criticized the generalization of the concept of national security by some countries and their blatant abuse of export control.

"Some countries are generalizing the concept of national security and abusing export control measures to add multiple enterprises to the so-called entity list and conduct long-arm jurisdiction," said Wang, the vice-minister of commerce.

# EXPORT CONTROLS BRIEFS

## BIS

### Chips Rules Add Macau

➤ This rule adds the destination of Macau to the scope of the Regional Stability (RS) controls that were implemented specific to China in the October 7 advanced computing and semiconductor manufacturing equipment rule. For purposes of the EAR, this rule does not change the status of Macau; it will continue to be treated as a separate destination from China. [88 FR 2821]

## CFIUS

### Truck Tech Transfer "Espionage"

➤ Members of the Committee on Foreign Investment in the US (CFIUS) have recommended the Justice Department file charges of economic espionage against the principals of a San Diego autonomous trucking startup, according to the *Wall Street Journal*.

TuSimple, which raised $1.25 billion in a public offering in April 2021 was funded principally by Sina Corp, according to Bloomberg. The recommendation for criminal charges, stemmed from concerns that two founders and the current chief executive of the company were improperly transferring technology to a Chinese entity.

## BIS

### Finalizes Wassenaar Implementation

➤ The December 2021 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) Plenary meeting made certain decisions affecting the WA control lists, which BIS is now implementing via amendments to the Commerce Control List.

On August 15, 2022, BIS published a final rule that implemented some of these decisions by adding to the CCL four technologies that met the criteria for emerging or foundational technologies under Section 1758 of the Export Control Reform Act of 2018 (ECRA).

This final rule implements the remaining controls agreed to during the December 2021 WA Plenary meeting by revising the CCL, as well as certain EAR provisions, including License Exception Adjusted Peak Performance (APP).

This final rule also makes corrections to align the scope of Significant Item (SI) license requirements throughout the EAR and makes a revision to License Exception Strategic Trade Authorization (STA). [88 FR 12108]