EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

September 1, 2024 - Volume 19, Issue 17

Hungarian National Arrested on Charges of Conspiring to Export U.S. Military-Grade Radios to Russian Government End Users -Monday, August 26, 2024

The Justice Department unsealed a criminal complaint charging Hungarian national Bence Horvath with violations of U.S. export controls targeting Russia, including by conspiring with others to illegally export U.S.-origin radio communications technology to Russian government end users without a license. Horvath is charged by complaint with one count of conspiring to violate the Export Control Reform Act of 2018 (ECRA). He was arrested on arrival at San Francisco International Airport in San Francisco, California, on Aug. 23.

"As alleged, the defendant attempted to purchase military-grade radios for Russian entities using a multinational procurement chain to evade law enforcement," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "The Justice Department remains committed to disrupting and holding accountable criminal networks that continue to fuel Russian aggression abroad and threaten our collective security."

"Targeting illicit global procurement networks that operate in the shadows to equip the Russian government is of the highest priority to BIS," said Assistant Secretary for Export Enforcement Matthew S. Axelrod of the Commerce Department's Bureau of Industry and Security (BIS). "As Horvath's arrest demonstrates, it doesn't matter where in the world you operate – when the United States believes your conduct violates our export laws, we take action."

"This defendant allegedly sought to skirt U.S. export controls put in place to protect our national security and to address Russia's unprovoked full-scale invasion of Ukraine," said U.S. Attorney Matthew M. Graves for the District of Columbia. "We will continue to work with our partners to bring to justice the people who scheme to secure U.S. technology in violation of U.S. laws."

According to the court documents, Horvath and others managed a multinational procurement network that contracted directly with various entities in the Russian government and worked on large scale projects such as the construction of operational radio communications systems in Russia's Kursk region along the Russian/Ukrainian border. The complaint alleges that Horvath himself arranged to purchase U.S.-origin radio communications technology and smuggle such technology to Russian government end-users through a network of affiliates located in Spain, Serbia, Hungary, Latvia, and elsewhere.

Beginning at least around January 2023, Horvath and others in his network initiated discussions with a small U.S. radio distribution company about procuring and exporting to Russia U.S.-manufactured military-grade radios and related accessories. Over the next several months, Horvath continued his efforts to secure those items, which he intended to transship to Russia via a freight forwarder in Latvia.

(*Continued On The Following Page)

NEWSLETTER NOTES

As part of the conspiracy, Horvath purchased 200 of the military-grade radios and intended to export them to Russia, but he was not successful. U.S. Customs and Border Protection detained the shipment, preventing the radios from falling into the hands of prohibited Russian end users.

Homeland Security Investigation, Defense Criminal Investigative Service and Department of Commerce are investigating the case.
Assistant U.S. Attorneys Christopher Tortorice and Maeghan Mikorski for the District of Columbia and Trial Attorney Sean Heiden of the National Security Division's Counterintelligence and Export Control Section are prosecuting the case.

Today's actions were coordinated through the Justice and Commerce Departments' Disruptive Technology Strike Force and the Justice Department's Task Force KleptoCapture. The Disruptive Technology Strike Force is an interagency law enforcement strike force co-led by the Departments of Justice and Commerce designed to target illicit actors, protect supply chains and prevent critical technology from being acquired by authoritarian regimes and hostile nation states. Task Force KleptoCapture is an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export restrictions and economic countermeasures that the United States has imposed, along with its allies and partners, in response to Russia's unprovoked military invasion of Ukraine.

A complaint is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated August 26, 2024
****

The breach, which includes Social Security numbers, could power a raft of identity theft, one expert says - by John Healey for LATimes.com

About four months after a notorious hacking group claimed to have stolen an extraordinary amount of sensitive personal information from a major data broker, a member of the group has reportedly released most of it for free on an online marketplace for stolen personal data.

The breach, which includes Social Security numbers and other sensitive data, could power a raft of identity theft, fraud and other crimes, said Teresa Murray, consumer watchdog director for the U.S. Public Information Research Group.

"If this in fact is pretty much the whole dossier on all of us, it certainly is much more concerning" than prior breaches, Murray said in an interview. "And if people weren't taking precautions in the past, which they should have been doing, this should be a five-alarm wake-up call for them."

According to a class-action lawsuit filed in U.S. District Court in Fort Lauderdale, Fla., the hacking group USDoD claimed in April to have stolen personal records of 2.9 billion people from National Public Data, which offers personal information to employers, private investigators, staffing agencies and others doing background checks. The group offered in a forum for hackers to sell the data, which included records from the United States, Canada and the United Kingdom, for $3.5 million, a cybersecurity expert said in a post on X. The lawsuit was reported by Bloomberg Law.

(*Continued On The Following Column)

Last week, a purported member of USDoD identified only as Felice told the hacking forum that they were offering "the full NPD database," according to a screenshot taken by BleepingComputer. The information consists of about 2.7 billion records, each of which includes a person's full name, address, date of birth, Social Security number and phone number, along with alternate names and birth dates, Felice claimed.

National Public Data didn't respond to a request for comment, nor has it formally notified people about the alleged breach. It has, however, been telling people who contacted it via email that "we are aware of certain third-party claims about consumer data and are investigating these issues."

In that email, the company also said that it had "purged the entire database, as a whole, of any and all entries, essentially opting everyone out." As a result, it said, it has deleted any "non-public personal information" about people, although it added, "We may be required to retain certain records to comply with legal obligations."
Several news outlets that focus on cybersecurity have looked at portions of the data Felice offered and said they appear to be real people's actual information. If the leaked material is what it's claimed to be, here are some of the risks posed and the steps you can take to protect yourself.

The threat of ID theft
The leak purports to provide much of the information that banks, insurance companies and service providers seek when creating accounts — and when granting a request to change the password on an existing account.

A few key pieces appeared to be missing from the hackers' haul. One is email addresses, which many people use to log on to services. Another is driver's license or passport photos, which some governmental agencies rely on to verify identities.

Still, Murray of PIRG said that bad actors could do "all kinds of things" with the leaked information, the most worrisome probably being to try to take over someone's accounts — including those associated with their bank, investments, insurance policies and email. With your name, Social Security number, date of birth and mailing address, a fraudster could create fake accounts in your name or try to talk someone into resetting the password on one of your existing accounts.

"For somebody who's really suave at it," Murray said, "the possibilities are really endless."

It's also possible that criminals could use information from previous data breaches to add email addresses to the data from the reported National Public Data leak. Armed with all that, Murray said, "you can cause all kinds of chaos, commit all kinds of crimes, steal all kinds of money.

How to protect yourself
Data breaches have been so common over the years, some security experts say sensitive information about you is almost certainly available in the dark corners of the internet. And there are a lot of people capable of finding it; VPNRanks, a website that rates virtual private network services, estimates that 5 million people a day will access the dark web through the anonymizing TOR browser, although only a portion of them will be up to no good.

(*Continued On The Following Page)

If you suspect that your Social Security number or other important identifying information about you has been leaked, experts say you should put a freeze on your credit files at the three major credit bureaus, Experian, Equifax and TransUnion. You can do so for free, and it will prevent criminals from taking out loans, signing up for credit cards and opening financial accounts under your name. The catch is that you'll need to remember to lift the freeze temporarily if you are obtaining or applying for something that requires a credit check.

Placing a freeze can be done online or by phone, working with each credit bureau individually. PIRG cautions never to do so in response to an unsolicited email or text purporting to be from one of the credit agencies — such a message is probably the work of a scammer trying to dupe you into revealing sensitive personal information.

For more details, check out PIRG's step-by-step guide to credit freezes.

You can also sign up for a service that monitors your accounts and the dark web to guard against identity theft, typically for a fee. If your data is exposed in a breach, the company whose network was breached will often provide one of these services for free for a year or more.

If you want to know whether you have something to worry about, multiple websites and service providers such as Google and Experian can scan the dark web for your information to see whether it's out there. But those aren't specific to the reported National Public Data breach. For that information, try a free tool from the cybersecurity company Pentester that offers to search for your information in the breached National Public Data files. Along with the search results, Pentester displays links to the sites where you can freeze your credit reports.

As important as these steps are to stop people from opening new accounts in your name, they aren't much help protecting your existing accounts. Oddly enough, those accounts are especially vulnerable to identity thieves if you haven't signed up for online access to them, Murray said — that's because it's easier for thieves to create a login and password while pretending to be you than it is for them to crack your existing login and password.

Of course, having strong passwords that are different for every service and changed periodically helps. Password manager apps offer a simple way to create and keep track of passwords by storing them in the cloud, essentially requiring you to remember one master password instead of dozens of long and unpronounceable ones. These are available both for free (such as Apple's iCloud Keychain) and for a fee.

Beyond that, experts say it's extremely important to sign up for two-factor authentication. That adds another layer of security on top of your login and password. The second factor is usually something sent or linked to your phone, such as a text message; a more secure approach is to use an authenticator app, which will keep you secure even if your phone number is hijacked by scammers.

(*Continued On The Following Column)

Yes, scammers can hijack your phone number through techniques called SIM swaps and port-out fraud, causing more identity-theft nightmares. To protect you on that front, AT&T allows you to create a passcode restricting access to your account; T-Mobile offers optional protection against your phone number being switched to a new device, and Verizon automatically blocks SIM swaps by shutting down both the new device and the existing one until the account holder weighs in with the existing device.

Your worst enemy may be you

As much or more than hacked data, scammers also rely on people to reveal sensitive information about themselves. One common tactic is to pose as your bank, employer, phone company or other service provider with whom you've done business and then try to hook you with a text or email message.

Banks, for example, routinely tell customers that they will not ask for their account information by phone. Nevertheless, scammers have coaxed victims into providing their account numbers, logins and passwords by posing as bank security officers trying to stop an unauthorized withdrawal or some other supposedly urgent threat.
People may even get an official-looking email purportedly from National Public Data, offering to help them deal with the reported leak, Murray said. "It's not going to be NPD trying to help. It's going to be some bad guy overseas" trying to con them out of sensitive information, she said.

It's a good rule of thumb never to click on a link or call a phone number in an unsolicited text or email. If the message warns about fraud on your account and you don't want to simply ignore it, look up the phone number for that company's fraud department (it's on the back of your debit and credit cards) and call for guidance.

"These bad guys, this is what they do for a living," Murray said. They might send out tens of thousands of queries and get only one response, but that response could net them $10,000 from an unwitting victim. "Ten thousand dollars in one day for having one hit with one victim, that's a pretty good return on investment," she said. "That's what motivates them."

****

FOR IMMEDIATE RELEASE

August 26, 2024
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

BIS Imposes Penalty on Pennsylvania Company Streamlight, Inc. to Resolve Alleged Violations of the Antiboycott Regulations

WASHINGTON, D.C. - Today, the Department of Commerce's Bureau of Industry and Security (BIS) imposed a civil penalty of $44,750 against Streamlight, Inc. (Streamlight), a global manufacturer of portable lighting products located in Eagleville, Pennsylvania, to resolve three alleged violations of the antiboycott provisions of the Export Administration Regulations (EAR). Streamlight voluntarily self-disclosed the conduct to BIS, cooperated with the investigation by BIS's Office of Antiboycott Compliance (OAC), and implemented remedial measures after discovering the conduct at issue, all of which resulted in a significant reduction in penalty.

(*Continued on the Following Page)

"Companies that do business with boycotting countries must be vigilant to ensure they detect prohibited boycott requests, report them to us, and decline to agree to them," said Assistant Secretary for Export Enforcement Matthew S. Axelrod. "When, as here, a freight forwarder asks you to certify that 'no labor, capital, parts or raw materials of Israeli origin have been used in the printing, publishing or manufacture of these goods,' the right response is to decline and to report the request – otherwise, there will be consequences."

Case Background:
As part of the settlement with BIS, Streamlight admitted to the conduct set forth in the Proposed Charging Letter, which alleged that Streamlight violated the antiboycott provisions of the EAR by furnishing information about its business relationships with boycotted countries or blacklisted persons and failing to report the receipt of a request to engage in a restrictive trade practice or foreign boycott against a country friendly to the United States. Specifically, Streamlight participated in a trade show in Bahrain in 2019. In connection with the shipment of goods for display at the trade show, the company furnished to its freight forwarder/logistics provider a commercial invoice/packing list certifying that the goods were not of Israeli origin and not manufactured by a company on the "Israeli Boycott Blacklist."

Furnishing such information is prohibited by Section 760.2(d) of the EAR. In addition, the company failed to report to BIS the receipt of the request to furnish this information, as required by Section 760.5 of the EAR.

The Order, Settlement Agreement, and Proposed Charging Letter are available here.

Additional Information:
These BIS actions were taken under the authority of the Anti-Boycott Act of 2018, a subpart of the Export Control Reform Act of 2018, and its implementing regulations, the EAR. The antiboycott provisions set forth in Part 760 of the EAR discourage, and in certain circumstances prohibit, U.S. persons from taking certain actions in furtherance or support of a boycott maintained by a foreign country against a country friendly to the United States (an unsanctioned foreign boycott).

In addition, U.S. persons must report to OAC their receipt of certain boycott-related requests, whether or not they intend to comply with them. Reports may be filed electronically or by mail on form BIS-621P for single transactions or on form BIS-6051P for multiple transactions involving boycott requests received in the same calendar quarter. U.S. persons located in the United States must postmark or electronically date stamp their reports by the last day of the month following the calendar quarter in which the underlying request was received. For U.S. persons located outside the United States, the postmark or date stamp deadline is the last day of the second month following the calendar quarter in which the request was received. Forms for both electronic transmission and mail submission may be accessed from the forms request page.

(*Continued on the Following Column)

BIS maintains a boycott Requester List on the OAC webpage with the objective of helping U.S. persons comply with the reporting requirements of the antiboycott regulations set forth in Part 760 of the EAR. Each entity on the Requester List has been recently reported to BIS on a boycott request report form, as required by Section 760.5 of the EAR, as having made a boycott-related request in connection with a transaction in the interstate or foreign commerce of the United States. U.S. persons are encouraged to diligently review transaction documents from all sources, but especially transaction documents with or involving these listed parties – given that they have been identified by others as a source of boycott-related requests – to identify possible boycott-related language and to determine whether U.S. person recipients have a reporting requirement to BIS pursuant to Part 760 of the EAR.

Pursuant to Section 764.8 of the EAR, a party may submit a voluntary self-disclosure if it believes that it may have violated Part 760 or Part 762 of the EAR (recordkeeping requirements relating to Part 760). More information on voluntary self-disclosures can be found online.

BIS has enhanced its antiboycott enforcement efforts to prevent U.S. companies from being used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel. In October 2022, BIS raised its penalties and instituted a requirement that companies entering into settlement agreements for antiboycott violations admit to a statement of facts outlining their conduct. In July 2023, BIS announced a renewed focus on foreign subsidiaries of U.S. companies and noted that it would explore additional ways to deter foreign parties from issuing or making boycott requests. BIS also modified the boycott reporting form to require submitters to indicate the identity of the requesting party.

For additional information regarding the application of the antiboycott provisions of the EAR, please contact OAC through the OAC Advice Line at (202) 482-2381 or through the online portal.

****

Gross Domestic Product (Second Estimate), Corporate Profits (Preliminary Estimate), Second Quarter 2024

Real gross domestic product (GDP) increased at an annual rate of 3.0 percent in the second quarter of 2024 (table 1), according to the "second" estimate released by the U.S. Bureau of Economic Analysis. In the first quarter, real GDP increased 1.4 percent.

The GDP estimate released today is based on more complete source data than were available for the "advance" estimate issued last month. In the advance estimate, the increase in real GDP was 2.8 percent. The update primarily reflected an upward revision to consumer spending (refer to "Updates to GDP").

The increase in real GDP primarily reflected increases in consumer spending, private inventory investment, and nonresidential fixed investment. Imports, which are a subtraction in the calculation of GDP, increased (table 2).

Compared to the first quarter, the acceleration in real GDP in the second quarter primarily reflected an upturn in private inventory investment and an acceleration in consumer spending. These movements were partly offset by a downturn in residential fixed investment. ***(*Continued On The Following Page)***

Current-dollar GDP increased 5.5 percent at an annual rate, or $383.2 billion, in the second quarter to a level of $28.65 trillion, an upward revision of $23.2 billion from the previous estimate (tables 1 and 3). More information on the source data that underlie the estimates is available in the "Key Source Data and Assumptions" file on BEA's website.

The price index for gross domestic purchases increased 2.4 percent in the second quarter, an upward revision of 0.1 percentage point from the previous estimate. The personal consumption expenditures (PCE) price index increased 2.5 percent, a downward revision of 0.1 percentage point. Excluding food and energy prices, the PCE price index increased 2.8 percent, a downward revision of 0.1 percentage point.

Personal Income

Current-dollar personal income increased $233.6 billion in the second quarter, a downward revision of $4.0 billion from the previous estimate. The increase primarily reflected increases in compensation and personal current transfer receipts (table 8).
Disposable personal income increased $183.0 billion, or 3.6 percent, in the second quarter, a downward revision of $3.2 billion from the previous estimate. Real disposable personal income increased 1.0 percent, unrevised from the prior estimate.

Personal saving was $686.4 billion in the second quarter, a downward revision of $34.1 billion from the previous estimate. The personal saving rate—personal saving as a percentage of disposable personal income—was 3.3 percent in the second quarter, a downward revision of 0.2 percentage point.

Gross Domestic Income and Corporate Profits

Real gross domestic income (GDI) increased 1.3 percent in the second quarter, the same as in the first quarter. The average of real GDP and real GDI, a supplemental measure of U.S. economic activity that equally weights GDP and GDI, increased 2.1 percent in the second quarter, compared with an increase of 1.4 percent in the first quarter (table 1).

Profits from current production (corporate profits with inventory valuation and capital consumption adjustments) increased $57.6 billion in the second quarter, in contrast to a decrease of $47.1 billion in the first quarter (table 10).

Profits of domestic financial corporations increased $46.4 billion in the second quarter, compared with an increase of $65.0 billion in the first quarter. Profits of domestic nonfinancial corporations increased $29.2 billion, in contrast to a decrease of $114.5 billion. Rest-of-the-world profits decreased $18.0 billion, in contrast to an increase of $2.3 billion. In the second quarter, receipts decreased $6.2 billion, and payments increased $11.8 billion

U.S. Support for the Philippines in the South China Sea

08/31/2024 06:28 PM EDT

Matthew Miller, Department Spokesperson

The United States stands with its ally, the Philippines, and condemns the dangerous and escalatory actions by the People's Republic of China (PRC) against lawful Philippine maritime operations in the vicinity of Sabina Shoal in the South China Sea on August 31. A China Coast Guard vessel deliberately collided three times with a Philippine Coast Guard vessel exercising its freedom of navigation in the Philippines' exclusive economic zone (EEZ), causing damage to the vessel and jeopardizing the safety of the crew onboard.

This is the latest in a series of dangerous and escalatory actions by the PRC. On multiple occasions throughout August 2024, the PRC has aggressively disrupted lawful Philippine aerial and maritime operations in the South China Sea, including at Sabina Shoal. The PRC's unlawful claims of "territorial sovereignty" over ocean areas where no land territory exists, and its increasingly aggressive actions to enforce them, threaten the freedoms of navigation and overflight of all nations.

The United State reiterates its call for the PRC to comport its claims and actions with international law and to desist from dangerous and destabilizing conduct.

The United States reaffirms that Article IV of the 1951 United States-Philippines Mutual Defense Treaty extends to armed attacks on Philippine armed forces, public vessels, or aircraft – including those of its Coast Guard – anywhere in the South China Sea.

****

Vietnam National Day

09/01/2024 04:39 PM EDT

Antony J. Blinken, Secretary of State

On behalf of the United States of America, I offer my best wishes to the people of Vietnam on your 79th National Day on September 2.
The United States supports a strong, prosperous, independent, and resilient Vietnam. This month, we also celebrate the first year of our Comprehensive Strategic Partnership, marking a historic new phase of U.S.-Vietnam cooperation. In honor of the legacy of General Secretary Nguyen Phu Trong, we recommit to respecting each other's independence, sovereignty, territorial integrity, and political systems. Furthermore, we look forward to fulfilling the commitments of our Comprehensive Strategic Partnership in areas of mutual importance, including economic cooperation, education, security, human rights, energy, environment, and health, and our shared desire for a free, open, prosperous, and peaceful Indo-Pacific Region. We also welcome the opportunity to jointly celebrate significant milestones in the year to come, including the 30th anniversary of the establishment of diplomatic relations between our two nations in 2025.

FOR IMMEDIATE RELEASE

August 23, 2024
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

COMMERCE TIGHTENS EXPORT CONTROLS, TARGETS ILLICIT PROCUREMENT NETWORKS FOR SUPPLYING RUSSIAN WAR MACHINE

WASHINGTON, D.C. – Today, the Commerce Department's Bureau of Industry and Security (BIS) is taking aggressive action to further restrict the supply of both U.S.-origin and "U.S. branded" (i.e., labeled) items to Russia and Belarus for the Kremlin's illegal war on Ukraine. Today's actions will further constrain Russia's ability to arm its military by targeting illicit procurement networks designed to circumvent global export controls.

Key actions include:

1. Further tightening controls on Russia by expanding the scope of the Russia/Belarus Military End User (MEU) and Procurement Foreign Direct Product (FDP) rule and imposing additional license requirements on operation software for computer numerically controlled (CNC) machine tools;
2. Cutting off exports to foreign companies on the BIS Entity List; applying the expanded Russia/Belarus MEU and Procurement FDP rule to dozens of entities outside Russia;
3. Restricting trade to additional foreign addresses and issuing guidance to exporters on identifying suspicious transactions related to foreign corporate service providers and listed foreign addresses, strengthening recently implemented restrictions on shell company addresses; and
4. Providing guidance and recommendations on contractual language referencing export regulations (the Export Administration Regulations, or EAR), specifically, restrictions that target unlawful reexports to Russia and Belarus.

"BIS has taken aggressive actions, in concert with our allies and partners, to impose strict export controls in response to Russia's illegal, unprovoked, and full-scale invasion of Ukraine. Today's action is an extension of this critical and ongoing work," **said Undersecretary of Commerce for Industry and Security Alan Estevez. "We will continue our** multilateral approach to attack this problem from all sides and use every tool in our arsenal to prevent Russia from gaining access to the advanced U.S. technology needed for its weapons."

Tightening Controls on Russia Expanding the scope of the existing FDP rule allows BIS export controls to capture entities outside Russia (and Belarus) that help procure not only U.S.-origin but also U.S.-branded items that support Russia's illegal, unjustified, and unprovoked war in Ukraine. This expansion is intended to target the transshipment of microelectronics and other items that bear the brand of a U.S.-headquartered company, even if manufactured outside the United States. Additionally, BIS is adding controls on certain software needed to operate CNC machine tools to prevent the provision of software updates to controlled tools in Russia and Belarus. This will have a delayed effective date of September 16, 2024.

(*Continued On The Following Column)

Entity List Additions
BIS is also adding 123 entities under 131 entries to the Entity List-- 63 entities in Russia or the Crimea Region of Ukraine, 42 in the People's Republic of China (PRC, including Hong Kong), and 14 entities in Türkiye, Iran, and Cyprus-- for shipping U.S.-origin and U.S.-branded items to Russia in contravention of U.S. export controls or for engaging in other activities contrary to U.S. national security and foreign policy interests. Since March 2022 (and including today's action), BIS has added 1,056 entries to the Entity List in response to Putin's February 2022 invasion of Ukraine and ongoing aggression against the country.

"Russia has been at the forefront of our policy decisions for the entirety of the Biden-Harris Administration. Our mandate is to use export controls to strategically and proactively address national security, technological, and political threats posed by our adversaries. This is especially true of Russia and its unjustified attacks in Ukraine," said **Assistant Secretary of Commerce for Export Administration, Thea D. Rozman Kendler.** "Today's action is an important step forward in bottlenecking the procurement networks Russia has turned to in the face of aggressive U.S. and allied export controls. We will not stop until Russia has nowhere to turn."

Targeting Shell Companies
In addition, BIS is further targeting diversion through shell companies by adding four high-diversion risk addresses in Hong Kong and Türkiye to the Entity List, thereby requiring a license for transactions involving parties using those addresses. BIS will continue to aggressively target entities around the world that ship U.S.-origin and U.S.-branded items to Russia.
Three addresses in Hong Kong and one address in Türkiye were added to the Entity List in connection with significant transshipment of sensitive items to Russia, building on changes made by a June 12, 2024 rule.

New Guidance for Exporters and Re-exporters
BIS is also issuing guidance and recommendations to U.S. exporters on language in sales contracts or other export documents involving items subject to the EAR to prevent diversion to Russia or Belarus.

Guidance to exporters on contract clauses: We are providing guidance to exporters regarding language they can include in their sales contracts or other export documents. Language used in these instances should ensure that overseas customers understand that BIS export controls under the EAR continue to apply to the items after the initial sale and that most items cannot be reexported to Russia without a license from BIS. This is similar to the European Union's "No re-export to Russia" clause, which requires EU companies to include similar language in certain sales contracts.

Guidance to foreign corporate service providers: Corporate service providers in places like Hong Kong or Türkiye provide their clients with a registered place of business – *i.e.*, an address they can use for billing or receiving goods. Although corporate service providers have legitimate business purposes, some bad actors use them to mask their identities and divert items to embargoed destinations or restricted parties. We are providing guidance to corporate service providers to help them avoid providing services to such bad actors – *e.g.*, screening against U.S. Government restricted parties lists and scrutinizing their customers who ship to Russia or to Iran and other embargoed destinations.

(*Continued On The Following Page)

Today's actions are taken in concert with similar actions by the Departments of State and the Treasury targeting Russian procurement networks in third countries around the world. U.S. export controls and sanctions have significantly impacted Russia's ability to build weapons systems for its unjustified war against Ukraine: Russia is forced to rely on lower-technology, often obsolete, foreign-produced items below the threshold of controls specified in multilateral export control regimes for its weapons systems and must pay two to four times pre-war prices for the key foreign-produced items it is able to obtain through complex, multi-hop procurement networks. Despite attempting to dramatically increase its military production, Russia still falls billions of dollars short in the imports needed to meet its stated production goals.

Additional Information:
In response to Russia's war against Ukraine, BIS imposed extensive sanctions on Russia and Belarus under the EAR effective February 2022. During the last two years, BIS has published a number of additional final rules strengthening the export controls on Russia and Belarus, including measures undertaken in coordination with the 38 U.S. allies and partners of the Global Export Control Coalition.

Taken together, these actions under the EAR reflect the U.S. government's position that Russia's war against Ukraine (with Belarus's complicity) flagrantly violates international law, is contrary to U.S. national security and foreign policy interests, and undermines global order, peace, and security.

Additional information on BIS's efforts to respond to Russia's war against Ukraine is available on BIS's website at: https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/russia-belarus.

Additional Background on the Entity List Process
The Entity List actions were taken under the authority of the Export Control Reform Act of 2018 and its implementing regulations, the Export Administration Regulations (EAR).

The Entity List (supplement no. 4 to part 744 of the EAR) identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States. Parties on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR.

Entity List additions are determined by the interagency End-User Review Committee (ERC), comprised of the Departments of Commerce (Chair), Defense, State, Energy, and where appropriate, the Treasury. The ERC makes decisions regarding additions to, removals from, or other modifications to the Entity List. The ERC makes all decisions to add an entity to the Entity List by majority vote and makes all decisions to remove or modify an entity by unanimous vote.

Additional information on the Entity List is available on BIS's website at: https://bis.doc.gov/index.php/policy-guidance/faqs

For additional information, please visit: www.bis.gov

New Measures to Degrade Russia's International Supply Chains and Wartime Economy

08/23/2024 02:38 PM EDT

Antony J. Blinken, Secretary of State

The United States is building on its unprecedented sanctions campaign and imposing new costs on those supporting Russia's war against Ukraine and its attempts to deny Ukraine's unique cultural identity. Today, one day ahead of the celebration of Ukrainian Independence Day, the United States is designating nearly 400 entities and individuals.

As part of today's actions, the Department of State is targeting those involved in sanctions evasion and circumvention, including entities in the People's Republic of China and those that support Russia's future energy production and exports.

We are also imposing sanctions on entities and individuals in both Russia and Belarus involved in the production of armed unmanned aerial vehicles, missiles, fighter aircraft, armored vehicles, defense electronics, and munitions that are being used to fuel Russia's war effort. We are also continuing to sanction those involved in the attempted 'Russification' and 're-education' of Ukraine's children.

Concurrently, the Department of the Treasury is targeting those facilitating support for Russia's military-industrial base, designating those involved in sanctions evasion on behalf of Russian oligarchs and malign cyber actors, and disrupting certain software and IT solutions essential to Russia's financial sector. Finally, the Department of Commerce is adding more than a hundred entries, including shell companies, to the Entity List for shipping U.S.-origin items to Russia in contravention of U.S. export controls.

We will continue to use all available tools to hinder Russia's use of the international financial system to wage its war of aggression and ensure Putin's invasion ends in strategic failure.

****

FOR IMMEDIATE RELEASE

August 26, 2024
www.bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

BIS Imposes Penalty on Pennsylvania Company Streamlight, Inc. to Resolve Alleged Violations of the Antiboycott Regulations

WASHINGTON, D.C. - Today, the Department of Commerce's Bureau of Industry and Security (BIS) imposed a civil penalty of $44,750 against Streamlight, Inc. (Streamlight), a global manufacturer of portable lighting products located in Eagleville, Pennsylvania, to resolve three alleged violations of the antiboycott provisions of the Export Administration Regulations (EAR). Streamlight voluntarily self-disclosed the conduct to BIS, cooperated with the investigation by BIS's Office of Antiboycott Compliance (OAC), and implemented remedial measures after discovering the conduct at issue, all of which resulted in a significant reduction in penalty.

(*Continued On The Following Page)

"Companies that do business with boycotting countries must be vigilant to ensure they detect prohibited boycott requests, report them to us, and decline to agree to them," said Assistant Secretary for Export Enforcement Matthew S. Axelrod. "When, as here, a freight forwarder asks you to certify that 'no labor, capital, parts or raw materials of Israeli origin have been used in the printing, publishing or manufacture of these goods,' the right response is to decline and to report the request – otherwise, there will be consequences."

Case Background:
As part of the settlement with BIS, Streamlight admitted to the conduct set forth in the Proposed Charging Letter, which alleged that Streamlight violated the antiboycott provisions of the EAR by furnishing information about its business relationships with boycotted countries or blacklisted persons and failing to report the receipt of a request to engage in a restrictive trade practice or foreign boycott against a country friendly to the United States. Specifically, Streamlight participated in a trade show in Bahrain in 2019. In connection with the shipment of goods for display at the trade show, the company furnished to its freight forwarder/logistics provider a commercial invoice/packing list certifying that the goods were not of Israeli origin and not manufactured by a company on the "Israeli Boycott Blacklist."

Furnishing such information is prohibited by Section 760.2(d) of the EAR. In addition, the company failed to report to BIS the receipt of the request to furnish this information, as required by Section 760.5 of the EAR.

The Order, Settlement Agreement, and Proposed Charging Letter are available here.

Additional Information:
These BIS actions were taken under the authority of the Anti-Boycott Act of 2018, a subpart of the Export Control Reform Act of 2018, and its implementing regulations, the EAR. The antiboycott provisions set forth in Part 760 of the EAR discourage, and in certain circumstances prohibit, U.S. persons from taking certain actions in furtherance or support of a boycott maintained by a foreign country against a country friendly to the United States (an unsanctioned foreign boycott).

In addition, U.S. persons must report to OAC their receipt of certain boycott-related requests, whether or not they intend to comply with them. Reports may be filed electronically or by mail on form BIS-621P for single transactions or on form BIS-6051P for multiple transactions involving boycott requests received in the same calendar quarter. U.S. persons located in the United States must postmark or electronically date stamp their reports by the last day of the month following the calendar quarter in which the underlying request was received. For U.S. persons located outside the United States, the postmark or date stamp deadline is the last day of the second month following the calendar quarter in which the request was received. Forms for both electronic transmission and mail submission may be accessed from the forms request page.

(*Continued On The Following Column)

BIS maintains a boycott Requester List on the OAC webpage with the objective of helping U.S. persons comply with the reporting requirements of the antiboycott regulations set forth in Part 760 of the EAR. Each entity on the Requester List has been recently reported to BIS on a boycott request report form, as required by Section 760.5 of the EAR, as having made a boycott-related request in connection with a transaction in the interstate or foreign commerce of the United States. U.S. persons are encouraged to diligently review transaction documents from all sources, but especially transaction documents with or involving these listed parties – given that they have been identified by others as a source of boycott-related requests – to identify possible boycott-related language and to determine whether U.S. person recipients have a reporting requirement to BIS pursuant to Part 760 of the EAR.

Pursuant to Section 764.8 of the EAR, a party may submit a voluntary self-disclosure if it believes that it may have violated Part 760 or Part 762 of the EAR (recordkeeping requirements relating to Part 760). More information on voluntary self-disclosures can be found online.

BIS has enhanced its antiboycott enforcement efforts to prevent U.S. companies from being used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel. In October 2022, BIS raised its penalties and instituted a requirement that companies entering into settlement agreements for antiboycott violations admit to a statement of facts outlining their conduct. In July 2023, BIS announced a renewed focus on foreign subsidiaries of U.S. companies and noted that it would explore additional ways to deter foreign parties from issuing or making boycott requests. BIS also modified the boycott reporting form to require submitters to indicate the identity of the requesting party.

For additional information regarding the application of the antiboycott provisions of the EAR, please contact OAC through the OAC Advice Line at (202) 482-2381 or through the online portal.

****

Press Releases

As Russia Feels Effects of Multilateral Sanctions Campaign, Treasury Takes Further Action Against Russia's International Supply Chains

August 23, 2024

One day ahead of Ukrainian Independence Day, Treasury continues implementation of G7 sanctions commitments in support of Ukraine

WASHINGTON — Building on the sanctions already imposed on Russia in response to its continued war of aggression against Ukraine, today the U.S. Department of the Treasury and the Department of State targeted nearly 400 individuals and entities both in Russia and outside its borders—including in Asia, Europe, and the Middle East—whose products and services enable Russia to sustain its war effort and evade sanctions. The United States government will continue to support Ukraine as it defends its independence and hold Russia accountable for its aggression.

(*Continued On The Following Page)

"Russia has turned its economy into a tool in service of the Kremlin's military industrial complex. Treasury's actions today continue to implement the commitments made by President Biden and his G7 counterparts to disrupt Russia's military-industrial base supply chains and payment channels," said Deputy Secretary of the Treasury Wally Adeyemo. "Companies, financial institutions, and governments around the world need to ensure they are not supporting Russia's military-industrial supply chains."

Treasury is targeting numerous transnational networks, including those involved in procuring ammunition and military materiel for Russia, facilitating sanctions evasion for Russian oligarchs through offshore trust and corporate formation services, evading sanctions imposed on Russia's cyber actors, laundering gold for a sanctioned Russian gold company, and supporting Russia's military-industrial base by procuring sensitive and critical items such as advanced machine tools and electronic components. Today's sanctions further limit Russia's future revenue from metals and mining. Treasury is also targeting Russian financial technology companies that provide necessary software and IT solutions for Russia's financial sector.

Treasury is aware of Russian efforts to facilitate sanctions evasion by opening new overseas branches and subsidiaries of Russian financial institutions. Foreign regulators and financial institutions should be cautious about any dealings with overseas branches or subsidiaries of Russian financial institutions, including efforts to open new branches or subsidiaries of Russian financial institutions that are not themselves sanctioned. Treasury has a range of tools available to respond to the establishment of new evasion channels.

The State Department is targeting entities and individuals involved in Russia's future energy, metals, and mining production and exports; sanctions evasion; Russia's military-industrial base, including armed unmanned aerial vehicle (UAV) production, Belarusian support for Russia's war effort, and air logistics entities; additional subsidiaries of State Atomic Energy Corporation Rosatom; and malign actors involved in the attempted, forcible "re-education" of Ukraine's children.

SANCTIONS EVASION, CIRCUMVENTION, AND BACKFILL

Consistent with commitments made by President Biden and G7 leaders, Treasury continues to target transnational networks that supply Russia with military materiel and sensitive dual-use goods like those included in the multilateral Common High Priority List, jointly developed by the United States, European Union, Japan, and the United Kingdom. Treasury is also targeting multiple networks that facilitate or enable illicit financial schemes and sanctions evasion on behalf of Russian revenue generators and oligarchs. Many of today's designations were enabled or informed by extensive coordination with Treasury's Financial Crimes Enforcement Network (FinCEN). Today's action targets almost a dozen distinct networks, designating more than 100 individuals and entities across 16 jurisdictions, including the People's Republic of China, Switzerland, Türkiye, and the United Arab Emirates.

For more information on these targets, please see Annex 1.

(*Continued On The Following Column)

RUSSIA'S TECHNOLOGICAL BASE

Today, Treasury is targeting more than 60 Russia-based technology and defense companies that are critical for the sustainment and development of Russia's defense industry, including entities involved in weapons development and modernization, automation and robotics, development and acquisition of dual-use electronics, digital surveillance, Internet of Things, and artificial intelligence. These sanctions target Russia's defense industry while protecting the access by Russian citizens to crucial telecommunications and other digital technology.

For more information on these targets, please see Annex 2.

LIMITING RUSSIA'S STRATEGIC METALS AND MINING SECTOR

Guided by commitments made by President Biden and G7 leaders to reduce Russia's revenues from metals, today Treasury is targeting entities involved in Russia's metals and mining sector, including steel, iron, and coal mining firms and auxiliary firms that provide specialized services to Russian metals and mining companies.

For more information on these targets, please see Annex 3.

RUSSIAN FINANCIAL TECHNOLOGY

Today, OFAC is targeting Russian financial technology companies as a part of implementing G7 commitments to curtail Russia's use of and access to the international financial system to further its war against Ukraine.

Atol is a Russian technology developer involved in services related to payments.

Centre of Financial Technologies Group (CFT)is one of the largest software companies in the Russian market. CFT provides an array of software products for banking and payment solutions for the Russian financial market.

Diasoft Ltd (Diasoft) is one of Russia's largest developers and suppliers of information technology (IT) solutions for the financial sector.

Atol, CFT, and Diasoft were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

ANNEX 1: SANCTIONS EVASION, CIRCUMVENTION, AND BACKFILL
Ammunition Procurement Network

Italian national **Giulio Sfoglietti** (Sfoglietti) has been involved in a procurement network involving a Türkiye facilitator to purchase more than $150 million worth of military equipment, ammunition, and ordnance for the Russian military from potential suppliers in Africa, Asia, the Caucasus, Central Asia, and Iran. Türkiye national **Hayri Tahirbeyoglu** (Tahirbeyoglu) is the Chairman of the Board of Directors of Türkiye-based ammunition, weapons, and military materiel company **Taha Savunma Sanayi Ve Ticaret Anonim Sirketi** (Taha Savunma) and has worked with Sfoglietti on the procurement of ammunition and weapons for likely Russian end-use. Sfoglietti has also worked to procure microelectronics and chips for Russia-based end-users.

(*Continued On The Following Page)

Sfoglietti associate Russian national **Marat Khanbalevich Gabitov** (Gabitov) has worked with an employee of U.S.-designated Russian defense conglomerate State Corporation Rostec to procure microelectronics related to radio frequency (RF) equipment. Gabitov has also worked to procure microelectronics, unmanned aerial vehicles (UAVs), and other machinery and equipment for Russia-based end-users.

Sfoglietti was designated pursuant to E.O. 14024 for operating or having operated in the defense and related materiel and technology sectors of the Russian Federation economy. Tahirbeyoglu and Taha Savunma were designated pursuant to E.O. 14024 for operating or having operated in the defense and related materiel sector of the Russian Federation economy. Gabitov was designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

Promtekh Supply Chain

U.S.-designated Russia-based Aktsionernoe Obshchestvo Promyshlennye Tekhnologii (Promtekh) has used a network of companies located in Türkiye, France, and Hong Kong to send high priority goods to Promtekh's subsidiaries. Russia-based **Aspectriym Limited Trade Development** (Aspectriym) is a subsidiary of Promtekh and is a defense procurement firm involved in the wholesale of electronic equipment and parts.

France-based **Industrial Technologies Group France** (ITGF) is a sister firm of U.S.-designated Promtechcomplekt JSC, a subsidiary of Promtekh, and has worked with Aspectriym to procure foreign- and U.S.-made electronic components. Hong Kong-based **Interasia Trading Group Limited** (Interasia Trading) is the sole owner of ITGF. Russian national **Igor Aleksandrovich Reutov** (Reutov) is the Executive Director of ITGF. Reutov is also the owner of Estonia-based **Free Sky Solutions OU** (Free Sky) and the Managing Partner of France-based **Aerialia**. Aerialia was established in January 2024.

ITGF also created a Türkiye-based firm, **Enutek Makina Sanayi ve Ticaret Limited Sirketi** (Enutek). Enutek has made hundreds of shipments of technology, including high priority dual-use technology such as electronic integrated circuits and ceramic capacitors, to U.S.-designated Promtekh subsidiaries, including Promtech Ulyanovsk, Dubna Switching Equipment Plant, and Promtech Irkutsk. Enutek was established in December 2022.

Other foreign suppliers to Promtekh subsidiaries include:

- Türkiye-based **Confienza Gida Pazarlama ve Ticaret Anonim Sirketi** (Confienza) has sent over 200 shipments to Aspectriym, with shipments including high priority dual-use technology.
- Hong Kong-based **Grun Group Co Limited** (Grun Group) has sent shipments totaling over $3 million to U.S.-designated subsidiaries of Promtekh, including shipments with high priority dual-use technology.
- Hong Kong-based **Hong Kong Yayang Trading Limited** (Yayang Trading) has sent shipments totaling over $9 million to U.S.-designated Promtekh subsidiaries Dubna Switching Equipment Plant and Aspectriym, with shipments including high priority dual-use technology.

(*Continued On The Following Column)

- Hong Kong-based **Kira International Trade Co Limited** (Kira International) is a partner of Aspectriym. Kira International has sent shipments totaling over $1.5 million to Aspectriym, with shipments including high priority dual-use technology.
- Hong Kong-based **Most Development Limited** (Most Development) has sent shipments totaling over $1 million to Aspectriym, with shipments including high priority dual-use technology.
- Hong Kong-based **New Wally Target International Trade Co Limited** (New Wally Target) has sent over $4 million worth of shipments to Aspectriym, with shipments including high priority dual-use technology.

Aspectriym, ITGF, Enutek, Interasia Trading, Reutov, Confienza, Grun Group, Yayang Trading, Kira International, Most Development, and New Wally Target were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy. Free Sky and Aerialia were designated pursuant to E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Reutov.

Sanctions Evasion Through Switzerland and Liechtenstein Trust and Corporate Services Providers

Swiss national **Anton Daniel Wyss** (Wyss) is a major enabler of Russian cash flow in Switzerland and Liechtenstein and has used his Liechtenstein-based trust and corporate services provider (TCSP) **Audax Consulting Trust Establishment** (Audax) to obfuscate Russian beneficial ownership and investments into foreign ventures. Through their co-owned Liechtenstein-based company **One Asset Management AG** (One Asset), Wyss and his Austrian national associate **Alexander Franz Josef Lins** (Lins) provide asset management and reallocation services to sanctioned Russian nationals. Lins uses his own TCSP, Liechtenstein-based **LMG Lighthouse Trust Reg** (LMG), to facilitate sanctions evasion schemes for Russian clients. Audax, One Asset, and LMG are all located at the same address, and both Audax and LMG advertise their services in Russian-language brochures. Austrian national **Stefan Anton Wolf** (Wolf) is a director of Audax.

Wyss, Audax, LMG, and Lins were designated pursuant to E.O. 14024 for operating or having operated in the trust and corporate formation services sector of the Russian Federation economy. Wolf was designated pursuant to E.O. 14024 for being or having been a leader, official, senior executive officer, or member of the board of directors of Audax. One Asset was designated pursuant to E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Wyss and Lins..

PRC-based Suppliers to Russia's Military-Industrial Base

The following entities were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy:

- Hong Kong-based machinery distributor **Smart Kit Technology Limited** (Smart Kit) has shipped high priority items, including chip-making machinery, to Russian companies including **Inzhiniring Grupp OOO** (Inzhiniring Grupp). Inzhiniring Grupp imports industrial machinery and equipment into Russia and has supplied manufacturing equipment to Russian government-owned labs.

(*Continued On The Following Page)

- Hong Kong-based **Siliborn Technology Limited** (Siliborn) is an electronic component distributor that has shipped high priority items, including electronic integrated circuits, to Russian companies, including U.S.-designated electronics company Staut Company Limited.
- Hong Kong and PRC-based **YLH Electronics HK Co Limited** has supplied high-priority goods, including electronic integrated circuits, to Russian company **Zakrytoe Aktsionernoe Obshchestvo Nauchno Vnedrencheskoe Predpriyatie Bolid**, a Russian manufacturer of sensors and security equipment.
- Hong Kong-based **Hongkong Chip Line International Co** has supplied high priority goods, including electronic integrated circuits, to U.S.-designated Russian microelectronics manufacturer Matriks Elektronika and Russian technology company **Maveriks**, another importer of high priority goods.
- Hong Kong-based **Hengye Tech Limited** has supplied high priority goods, including electronic integrated circuits, to Russian electronic components manufacturer **Elektroradiokomponenty Severo Zapad**.
- Hong Kong-based **LL Electronic Limited** has shipped electronic integrated circuits and multilayer ceramic capacitors to U.S.-designated Russian electronic component importer Limited Liability Company Kvazar.
- Hong Kong-based **Allchips Limited** has supplied high priority goods, including electronic integrated circuits, to **Limited Liability Company Micropribor**, a Russian wholesaler of electronic equipment.
- Hong Kong-based **Fepood Electronics HK Co Limited** has shipped electronic integrated circuits and multilayer ceramic capacitors to U.S.-designated Russian electronic components supplier LLC Spetselservis.
- Hong Kong-based Xin Quan Electronics Co Limited has made thousands of shipments of high priority goods, including electronic integrated circuits, to Russian company Snabinter, a Russian wholesaler of electronic equipment.
- PRC-based Jinhua Hairun Power Technology Co Ltd produces cutting machines, carburetors, and pistons and has made hundreds of shipments to Russia, including engine parts, transmissions, and gear components.
- Hong Kong-based Xin Quan Electronics Co Limited has made thousands of shipments of high priority goods, including electronic integrated circuits, to Russian company Snabinter, a Russian wholesaler of electronic equipment.
- PRC-based Jinhua Hairun Power Technology Co Ltd produces cutting machines, carburetors, and pistons and has made hundreds of shipments to Russia, including engine parts, transmissions, and gear components.
- Hong Kong-based Shenzhen Royo Technology Co Limited and PRC-based Qingdao Hehuixin International Trade Co Ltd have shipped technologies to U.S.-designated Russian defense company Limited Liability Company Drake, which is contracted to receive UAV parts, components, and materials from Iran for use in Iranian-designed, Russian-manufactured UAVs.

(*Continued On The Following Column)

- Hong Kong-based **HK Cinty Co Limited** (HK Cinty) has shipped electronic integrated circuits, multilayer ceramic capacitors, and electrical parts of machinery to Russia-based end-users. HK Cinty has sent over $2 million worth of goods to Russia-based end-users, with shipments including high priority goods. HK Cinty was established in July 2022.
- PRC-based **Foshan Golden Age Motor Technology Co., Ltd.** supplies technology, including electric drives and servo motors, to Russia-based **Limited Liability Company Mekhatronika**, a computer numerical control technology developer and importer of integrated circuits.
- Hong Kong-based **Asia Material Solutions Company Limited** (Asia Material) has shipped electronic integrated circuits to Russia-based end-users. Asia Material has sent shipments worth just under $1,000,000 to Russia-based end users. Asia Material has been identified as a cover company for Russian intelligence.

Fighter Jet Supply Network

Russia-based **Exiton** has imported foreign electronic components into Russia and supplies U.S.-designated Russian company Joint Stock Company Experimental Design Bureau named after A.S. Yakovlev, a manufacturer involved in the production of Sukhoi fighter jets. Russia-based **Limited Liability Company Eksiton** (Eksiton) imports high priority goods, including electronic integrated circuits. Hungary-based **Matrix Metal Group Korlatolt Felelossegu Tarsasag Felszamolas Alatt** (Matrix Metal) has supplied high priority goods, including electronic integrated circuits, to Eksiton. Additionally, Russia-based military contractor and developer of anti-aircraft systems **Aktsionernoe Obshchestvo Displei Komponent** (Displei Komponent) has received regular shipments of electronic components from both Matrix Metal and Cyprus-based **Noratec Holdings Ltd**.

Exiton, Eksiton, Matrix Metal, Displei Komponent, and Noratec Holdings Ltd were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy.

Alexandre Orloff

Swiss-Russian national **Alexandre Orloff** (Orloff) has been working with a Russian government covert procurement network for years to acquire high-value, foreign-made semiconductor-related equipment and technology for Russian military end-users. Orloff has also been part of a scheme to acquire specialized thermal cameras for a Russian end-user.

Orloff owns and is the director and secretary of an eponymous United Kingdom-based company, **Alexandre Orloff Ltd** (AO Ltd). AO Ltd, in turn, owns Hong Kong-based **Zvigeni Technological Systems Limited** (Zvigeni) and **Dougong Trading Hong Kong Limited** (Dougong) and Canada-based **9105 2829 Quebec Inc**. Orloff is also the founder and CEO of UAE-based **Digital Marketing Awards FZ LLC** (DMA).

(*Continued On The Following Page)

PRC-based **Shanghai Techinital Materials Co Ltd** (Shanghai Techinital), a producer of components for semiconductor manufacturing equipment, has made dozens of shipments to U.S.-designated Joint Stock Company Scan (JSC Scan), including of high priority dual-use technology such as signal generators and oscilloscopes. JSC Scan designs microelectronics and has its own center for designing integrated circuits. Shanghai Techinital has open contracts to provide JSC Scan with technology, despite the latter's designation. In 2023 alone, Zvigeni transmitted more than $1.5 million to Shanghai Techinital.

Orloff and Shanghai Techinital were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy. AO Ltd, Zvigeni, Dougong, 9105 2829 Quebec Inc, and DMA were designated pursuant to E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Orloff.

Russian Evasion of Cyber Sanctions

In June 2018, the Department of the Treasury sanctioned a network of entities working at the behest of the Russian Federation and its military and intelligence units to increase Russia's malicious cyber capabilities. Since that time, individuals associated with those entities, including **Ilya Medvedovsky** (Medvedovsky), **Dmitriy Evdokimov** (Evdokimov), **Yevgeniya Klimina** (Klimina), **Dmitriy Chastuhin** (Chastuhin), **Taranjeet Kambo** (Kambo), and **Gleb Cherbov** (Cherbov) have established, developed, and supported a complex network of technology companies to continue their work unimpeded. The front companies set up by these individuals, at times registered in the names of family members, operate primarily in the technology sector of the Russian Federation economy, with efforts being taken by individuals such as Chastuhin and Klimina, to establish a technology presence outside of Russia. Included in these companies is **OOO Soft Plyus**, a Russia-based firm that sells cyber security software and is formerly known as OOO Hexway, for whom Chastuhin has claimed to be the founder and CEO; **Cloudrun LLC**, a Russia-based company founded by Evdokimov that develops computer software; **Didzhital Komplaens, OOO** and **Kiber Servis, OOO**, both of which offer cyber security services and were founded by an individual believed to be related to Medvedovksy; **Didzhital Sekyuriti Servisis, OOO**; and **Machine Learning Labs S.R.O.**, founded and owned by Klimina. Medvedovsky, alongside Chastuhin, Cherbov, and Klimina, have been involved in decision making related to the operation of Soft Plyus and other related companies, whereas Kambo and Cherbov have worked together to service customers of Soft Plyus.

Medvedovsky, Klimina, OOO Soft Plyus, Cloudrun LLC, Didzhital Komplaens, OOO, Didzhital Sekyuriti Servisis, OOO, and Kiber Servis, OOO, were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy. Chastuhin was designated pursuant to E.O. 14024 for being or having been a leader, official, senior executive officer, or member of the board of directors of OOO Soft Plyus. Evdokimov was designated pursuant to E.O. 14024 for being or having been a leader, official, senior executive officer, or member of the board of directors of Cloudrun LLC. Cherbov and Kambo were designated pursuant to E.O. 14024 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, OOO Soft Plyus. Machine Learning Labs S.R.O. was designated pursuant to E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Klimina.

(*Continued On The Following Column)

Alikhanov Machine Tool Procurement

Italy-based machine tool manufacturer **Fagima Fresatrici SPA** (Fagima) has worked closely with U.S.-designated Russian procurement agent Dmitrii Vladimirovich Alikhanov (Alikhanov) to facilitate the shipment of Fagima-produced machines through various third-country intermediary companies for Russian defense end-users. Fagima's owner and CEO **Massimo Falchini** (Falchini) and Fagima marketing executive **Fulvio Salvadori** (Salvadori) have helped fulfill orders for Alikhanov's network and evade sanctions, including after Alikhanov's designation in June 2024.

Fagima, Falchini, and Salvadori were designated pursuant to E.O. 14024 for operating or having operated in the manufacturing sector of the Russian Federation economy.

Illicit Russian Gold Trade

UAE-based, UK-sanctioned **Paloma Precious DMCC** (Paloma Precious) is a precious metals trading firm that has helped move Russian gold abroad. Paloma Precious and U.S.-designated Taube Precious HK Limited played a key role in numerous illicit Russian gold trading and laundering schemes, including with U.S.-designated Andrey Dmitriyevich Sudakov (Sudakov). Sudakov, an employee of U.S.-designated Russian gold producer Public Joint Stock Company Polyus, and his Hong Kong-based associate Mu Xiaolu (Mu), engaged in a complex, multi-layered laundering scheme whereby payments from the sale of Russian-origin gold were converted into fiat currency and cryptocurrencies through numerous UAE and Hong Kong-based front companies.

UAE-based Russian national **Vladislav Faridovich Guzey** (Guzey) has worked closely with Sudakov and Mu to launder proceeds of Russian-origin gold through UAE- and Hong-Kong based entities. As part of their effort to move Russia-origin gold, Sudakov and Mu utilized UAE-based front companies **Shams Gold Trading FZE** (Shams) and **Swiss Luxury FZE** (Swiss Luxury), and Hong Kong-based front companies **Universal Gold Hong Kong Limited** (Universal Gold) and **Bright Universe International Limited** (Bright Universe).

UAE-based **Trio Jewells LLC** (Trio) has made dozens of shipments of precious metal ingots to and from a Russia-based precious metals producer and processor.

Paloma Precious, Guzey, Shams, Swiss Luxury, Universal Gold, Bright Universe, and Trio were designated pursuant to E.O. 14024 for operating or having operated in the metals and mining sector of the Russian Federation economy.

Petrov Covert Procurement

Türkiye-based **Whitestone Bilism Tic Ve Sanayi Ltd Sti** (Whitestone) is owned by U.S.-designated Evgenii Stanislavich Petrov (Petrov) and has been used by Petrov to process payments for Petrov's procurement activity for Russian end-users linked to Russia's intelligence services. Petrov has acted as a covert procurement intermediary and has worked to obtain export-controlled foreign-made products on behalf of Russian-end-users. Whitestone was established in October 2023. Treasury also previously designated Türkiye-based MSO Lojistik Tic Ve Sanayi Ltd Sti for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Petrov.

(*Continued On The Following Page)

Whitestone was designated for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Petrov, a person whose property and interest in property are blocked pursuant to E.O. 14024.

Dalkos

Russia-based machinery and spare parts provider **Dalkos Co Ltd** (Dalkos) has orchestrated a transnational sanctions evasion scheme to deceive foreign machinery manufacturers into inadvertently sending machine tools into Russia via third countries. Dalkos customers include Russian companies that produce drones, tanks, and air defense units. Dalkos co-owners **Konstantin Svyatoslavovich Kalinov** (Kalinov) and **Aleksandr Aleksandrovich Pushkov** (Pushkov) also own Estonia-based **SPE OU**, which Dalkos has used to acquire millions of dollars of goods.

Dalkos, Kalinov, and Pushkov were designated pursuant to E.O. 14024 for operating or having operated in the manufacturing sector of the Russian Federation economy. SPE OU was designated pursuant to E.O. 14024 for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, Kalinov and Pushkov.

Türkiye-based Manufacturing Equipment Suppliers

Türkiye-based **Hidropark Hidrolik Pnomatik San Ve Tic Ltd Sti** (Hidropark) sells hydraulic and pneumatic equipment and has supplied computer numerical control (CNC) machine tools and machining centers to Russian end-users. Hidropark has sent shipments totaling over $800,000 to Russia-based end-users, which is more than its reported annual revenue.

Turkiye-based **Feva Dis Ticaret Limited Sirketi** (Feva) has supplied CNC machine tools to Russian end-users. Feva has sent over 500 shipments to Russia-based end-users, with shipments including manufacturing equipment. U.S.-designated Russian firm Limited Liability Company AK Microtech sought to evade sanctions by purchasing goods through Feva. Feva was established in April 2022. Hidropark and Feva were designated pursuant to E.O. 14024 for operating or having operated in the manufacturing sector of the Russian Federation economy.

Technopole Procurement Network

On December 22, 2022, the U.S. Department of State designated Technopole Company (Technopole) and the P.P. Shirshov Institute of Oceanology of the Russian Academy of Sciences (Shirshov Institute) pursuant to E.O. 14024 for operating or having operated in the marine sector of the Russian Federation economy. Technopole produces a navigation system for the use of Russian military vessels and provides equipment for a variety of ocean exploration, oceanology, oceanography, and hydrography activities, among others. The Shirshov Institute is the largest Russian oceanology research center. The Shirshov Institute also develops remotely operated and autonomous robotic tools that support the surface and submarine forces of the Russian navy and other Russian government agencies. Russian national **Alexander Petrovich Voronkov** (Voronkov) has been the Director of Technopole since 2007 and is the 100 percent owner of the company. Russian national **Viktor Georgiyevich Spiridonov** (Spiridonov) is the Deputy Director of Technopole and is actively involved in Russian procurement of western-origin equipment.

(*Continued On The Following Column)

Idronaut S.R.L. (Idronaut) is one of Technopole's foreign partners and facilitates the procurement and sale of equipment, on behalf of Technopole and other Russian military end users, including the Shirshov Institute. **Flavio Graziottin** (Graziottin) owns Idronaut and has worked to circumvent U.S. and European Union sanctions through Idronaut to acquire equipment for Technopole.

Idronaut and PRC-based company **Shanghai Oceanen Environmental Science and Technology Co.** (Shanghai Oceanen) have worked to circumvent sanctions on Technopole and have procured equipment on Technopole's behalf. Shanghai Oceanen is the distributor for Idronaut in the PRC and has acted as a middleman to ship Idronaut's equipment to Technopole and the Shirshov Institute. Shanghai Oceanen has historically assisted Technopole in procuring dual-use equipment for Russian end users. In early 2023, Shanghai Oceanen sent a shipment to Technopole containing surveying equipment, including hydrographic, oceanographic, hydrological, meteorological, or geophysical instruments and appliances. PRC national **Liu Yang** is the Technical Director for Shanghai Oceanen and uses the company to facilitate the procurement of foreign equipment.

Russia-based **Technomar** offers advanced measurement oceanographic and hydrographic equipment in the fields of oceanography and hydrology from the world's leading manufacturers.

Voronkov and Spiridonov were designated pursuant to E.O. 14024 for having acted or purported to act for or on behalf of, directly or indirectly, Technopole. Idronaut was designated pursuant to E.O.14024 for having materially assisted, sponsored, or provided financial, material, technological or other support for, or goods or services in support of, Technopole and the Shirshov Institute. Graziottin was designated pursuant to E.O. 14024 for having acted or purported to act for or on behalf of, directly or indirectly, Idronaut. Shanghai Oceanen was designated pursuant to E.O. 14024 for having materially assisted, sponsored, or provided financial, material, technological or other support for, or goods or services in support of, Technopole. Liu Yang was designated pursuant to E.O.14024 for having acted or purported to act for or on behalf of, directly or indirectly, Shanghai Oceanen. Technomar was designated pursuant to E.O. 14024 for operating or having operated in the marine sector of the Russian Federation economy.

ANNEX 2: RUSSIA'S DOMESTIC WAR ECONOMY

The following Russia-based persons were designated pursuant to E.O. 14024 for operating or having operated in the defense and related materiel sector of the Russian Federation economy:

- **46th Central Research and Development Institute of the Ministry of Defense** (46th CRDI) is a Russian Ministry of Defense (MoD) research organization that develops systems to modernize Russia's weapons. The 46th CRDI also studies electronic warfare and military applications of artificial intelligence.
- **Federal State Governmental Institution 4 Central Research Institute of the Ministry of Defense of the Russian Federation** (4CRI) is a Russian entity involved in the development and implementation of dual-use technologies in the creation of new types of weapons. 4CRI provides scientific and technical support for missile systems.

(*Continued On The Following Page)

- **Federal State Governmental Institution 27 Central Research Institute of the Ministry of Defense of the Russian Federation** is a Russian MoD scientific research institute that conducts military scientific research, provides military scientific support for the creation of automated systems and complexes, and creates samples of military equipment.
- **Joint Stock Company KT – Unmanned Systems** (KT – Unmanned Systems) cooperates with the Russian MoD and U.S.-designated Federal Security Service (FSB). KT – Unmanned Systems supports software used for Russian weapons development.
- **Joint Stock Company Special Design Bureau of the Russian Ministry of Defense** develops unmanned robotic combat vehicles.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Konstruktorskoe Byuro Vostok** is the developer of the Scalpel UAV, which is used by Russian forces in Ukraine such as the Vostok Battalion. The Scalpel UAV is a one-way-attack platform that can be equipped with a payload weighing up to five kilograms.
- **Prikladnye Tekhnologii** has indicated a willingness to procure Chinese-origin engines with cruise missile applications for the Russian weapons sector.
- **Tekhekspertiza AO** has worked with the Russian weapons sector to arrange the purchase of engines with cruise missile applications.
- TRV Engineering JSC is the official authorized procurement agent for Russia's U.S.-designated Tactical Missiles Corporation (KTRV) and its subordinate companies. TRV Engineering JSC receives a commission for goods supplied, work performed, and services provided to KTRV, its subordinates, and other members of Russia's defense industrial base. TRV Engineering JSC has been directly involved with supplying products and services in support of Russian state defense orders, including providing machine tools to KTRV subordinates such as U.S.-designated State Machine-Building Design Bureau Raduga. TRV Engineering JSC's General Director Mikhail Vladimirovich Kolesnikov was directly involved with fulfilling TRV Engineering JSC's state defense orders and other procurements in the interest of companies in the Russian defense industrial base.

Russia-based electronic parts wholesaler **LLC Semicor** is a subsidiary of U.S.-designated LLC Laser Components (Laser Components). LLC Semicor has offered to supply engines on behalf of LLC Laser Components in support of Russian cruise missile development. LLC Semicor was designated pursuant to E.O. 14024 for having materially assisted, sponsored, or provided material, financial, or technological support for, or goods or services to or in support of, Laser Components.

The following Russia-based persons were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy:

- **Aktsionernoe Obshchestvo Korporatsiya Galaktika** develops digitalization platforms, including for U.S.-designated Russian defense giants Rostec and Uralvagonzavod.

(*Continued On The Following Column)

- **Aktsionernoe Obshchestvo Opytnoe Konstruktorskoe Byuro Eksiton** is involved in experimental design work and research with the Russian MoD, including related to the assembly of microcircuits.
- **Aktsionernoe Obshchestvo Zavod Rekond** specializes in the production of electronic components, microcircuits, and semiconductor devices, particularly sensitive dual-use devices such as ceramic and tantalum capacitors.
- **AO NPP SAIT** (Sait), a producer of technology such as memory units, has received Russian state funding and is involved in the manufacture of computers and peripheral equipment. Sait works with U.S.-designated Russian defense entity Federal State Institution of Higher Vocational Education Moscow Institute of Physics and Technology, which has been recognized by the Russian MoD for developing technologies in the interest of Russia's military.
- **Autonomous Non Profit Organization Artificial Intelligence Research Institute** conducts research in the field of artificial intelligence and has developed neural networks related to unmanned vehicles.
- **Elprom Limited Liability Company** supplies microcircuits and other electronic components, including to a Russian UAV producer.
- **Federal State Budgetary Institution Technological Institution for Superhard and Novel Carbon Materials** develops advanced manufacturing technologies and high-tech components used by several U.S.-designated Russian defense entities.
- **Federal State Institution Federal Research Center Informatics and Management of the Russian Academy of Sciences** (FRC CSC RAS) conducts research and development in the fields of computer science, informational technology, and systems analysis. A FRC CSC RAS researcher has developed mathematical modeling technology for analyzing financial flows for Russia's military-industrial base.
- Aktsionernoe Obshchestvo Korporatsiya Galaktika develops digitalization platforms, including for U.S.-designated Russian defense giants Rostec and Uralvagonzavod.
- Aktsionernoe Obshchestvo Opytnoe Konstruktorskoe Byuro Eksiton is involved in experimental design work and research with the Russian MoD, including related to the assembly of microcircuits.
- Aktsionernoe Obshchestvo Zavod Rekond specializes in the production of electronic components, microcircuits, and semiconductor devices, particularly sensitive dual-use devices such as ceramic and tantalum capacitors.
- AO NPP SAIT (Sait), a producer of technology such as memory units, has received Russian state funding and is involved in the manufacture of computers and peripheral equipment. Sait works with U.S.-designated Russian defense entity Federal State Institution of Higher Vocational Education Moscow Institute of Physics and Technology, which has been recognized by the Russian MoD for developing technologies in the interest of Russia's military.

(*Continued On The Following Page)

- **Autonomous Non Profit Organization Artificial Intelligence Research Institute** conducts research in the field of artificial intelligence and has developed neural networks related to unmanned vehicles.
- **Elprom Limited Liability Company** supplies microcircuits and other electronic components, including to a Russian UAV producer.
- **Federal State Budgetary Institution Technological Institution for Superhard and Novel Carbon Materials** develops advanced manufacturing technologies and high-tech components used by several U.S.-designated Russian defense entities.
- **Federal State Institution Federal Research Center Informatics and Management of the Russian Academy of Sciences** (FRC CSC RAS) conducts research and development in the fields of computer science, informational technology, and systems analysis. A FRC CSC RAS researcher has developed mathematical modeling technology for analyzing financial flows for Russia's military-industrial base.
- **FGUP PO Oktyabr**, one of the largest radio-electronics companies in Russia, produces radar systems.
- **Joint Stock Company 31 State Design Institute for Special Construction** (31 State Design Institute) designs complex antenna systems, radio equipment, radio electronic equipment, and facilities with network computer control systems, information security systems, and intrusion protection and detection systems. 31 State Design Institute has built central and command posts for the Russian MoD.
- **Joint Stock Company Akmetron** (Akmetron) develops and produces electronics and specialized software. Akmetron has procured dual-use technology for a Russian UAV producer.
- Autonomous Non Profit Organization Artificial Intelligence Research Institute conducts research in the field of artificial intelligence and has developed neural networks related to unmanned vehicles.
- Elprom Limited Liability Company supplies microcircuits and other electronic components, including to a Russian UAV producer.
- Federal State Budgetary Institution Technological Institution for Superhard and Novel Carbon Materials develops advanced manufacturing technologies and high-tech components used by several U.S.-designated Russian defense entities.
- Federal State Institution Federal Research Center Informatics and Management of the Russian Academy of Sciences (FRC CSC RAS) conducts research and development in the fields of computer science, informational technology, and systems analysis. A FRC CSC RAS researcher has developed mathematical modeling technology for analyzing financial flows for Russia's military-industrial base.
- FGUP PO Oktyabr, one of the largest radio-electronics companies in Russia, produces radar systems.
- Joint Stock Company 31 State Design Institute for Special Construction (31 State Design Institute) designs complex antenna systems, radio equipment, radio electronic equipment, and facilities with network computer control systems, information security systems, and intrusion protection and detection systems. 31 State Design Institute has built central and command posts for the Russian MoD.
- Joint Stock Company Akmetron (Akmetron) develops and produces electronics and specialized software. Akmetron has procured dual-use technology for a Russian UAV producer.

(*Continued On The Following Column)

- **Kribrum JSC** develops hardware and software for monitoring social media and has signed a contract with the Russian Government's main censorship body to automate internet monitoring.
- **Kugel Limited Liability Company** develops robotic solutions for welding.
- **Limited Liability Company 4Test** has imported high-priority items, including high-value electronics and manufacturing, production, and quality testing equipment for electronics components, circuit boards, and modules.
- **Limited Liability Company Afinor** supplies control-measurement equipment and software and has contracted with the Government of the Russian Federation for missile-related activities.
- **Limited Liability Company Alfa Instruments** imports and wholesales high priority goods, such as oscillographs and signals generators, including to the U.S.- designated Institute of Laser Physics of the Siberian Branch of the Russian Academy of Sciences.
- **Limited Liability Company Eksikyushn Er Di Si** (Execution RDC) operates in the field of enterprise automation. Execution RDC works with Russia's main censor on a neural network that uses artificial intelligence to scan the Internet.
- **Limited Liability Company ETM Photonics** imports high priority goods, including integrated circuits, and a wholesaler of technology, including through Russian state procurement contracts.
- **Limited Liability Company Khaverim** wholesales electronic equipment and has imported high priority electronics, such as electronic integrated circuits, into Russia.
- Limited Liability Company Head Point provides an Internet of Things (IoT) platform that can be used by law enforcement and supports Russian government surveillance systems.
- Limited Liability Company Palitrumlab (Palitrumlab) develops machine-learning and linguistics algorithms and software that can be used to monitor social networks and social media. Palitrumlab is involved in Russian censorship activities.
- Limited Liability Company Vektor Iks (Vektor Iks) develops neural networks and algorithms that are used in Russian censorship activities.
- Limited Liability Company Intem Lab (InTheme) specializes in the digitalization of logistics processes. InTheme provides business process automation services to several U.S.-designated Russian entities.
- Limited Liability Company Green Chip supplies radio-electronic components for the development, production, and repair of industrial, special-purpose, and energy enterprises.
- Kribrum JSC develops hardware and software for monitoring social media and has signed a contract with the Russian Government's main censorship body to automate internet monitoring.
- Kugel Limited Liability Company develops robotic solutions for welding.
- Limited Liability Company 4Test has imported high-priority items, including high-value electronics and manufacturing, production, and quality testing equipment for electronics components, circuit boards, and modules.
- Limited Liability Company Afinor supplies control-measurement equipment and software and has contracted with the Government of the Russian Federation for missile-related activities. ***(*Continued On The Following Page)***

- **Limited Liability Company Tsifra** (Zyfra) develops and implements industrial digital solutions. The Zyfra Industrial IoT platform has been used by U.S.-designated military engine producer Joint Stock Company United Engine Corporation to monitor production and simulate testing for turbo jets for a combat-capable trainer aircraft.
- **Limited Liability Company Dronoport**, using the trade name "HIVE," develops autonomous drone solutions for monitoring and has developed a neural network to analyze input data, including thermal imagery and special indicators.
- **Limited Liability Company PT Elektronik** is an electronics distributor that has supplied a Russian UAV producer.
- **Limited Liability Company Simbirskoe Konstruktorskoe Byuro Piranya** is a computer programming company that develops drones used by Russia's military.
- **Limited Liability Company Amitron Elektroniks** produces military-certified coaxial radio components.
- Limited Liability Company Tsifra (Zyfra) develops and implements industrial digital solutions. The Zyfra Industrial IoT platform has been used by U.S.-designated military engine producer Joint Stock Company United Engine Corporation to monitor production and simulate testing for turbo jets for a combat-capable trainer aircraft.
- Limited Liability Company Dronoport, using the trade name "HIVE," develops autonomous drone solutions for monitoring and has developed a neural network to analyze input data, including thermal imagery and special indicators.
- Limited Liability Company PT Elektronik is an electronics distributor that has supplied a Russian UAV producer.
- Limited Liability Company Simbirskoe Konstruktorskoe Byuro Piranya is a computer programming company that develops drones used by Russia's military.
- Limited Liability Company Amitron Elektroniks produces military-certified coaxial radio components.
- Limited Liability Company Tsifra (Zyfra) develops and implements industrial digital solutions. The Zyfra Industrial IoT platform has been used by U.S.-designated military engine producer Joint Stock Company United Engine Corporation to monitor production and simulate testing for turbo jets for a combat-capable trainer aircraft.
- Limited Liability Company Dronoport, using the trade name "HIVE," develops autonomous drone solutions for monitoring and has developed a neural network to analyze input data, including thermal imagery and special indicators.
- Limited Liability Company PT Elektronik is an electronics distributor that has supplied a Russian UAV producer.
- Limited Liability Company Simbirskoe Konstruktorskoe Byuro Piranya is a computer programming company that develops drones used by Russia's military.
- Limited Liability Company Amitron Elektroniks produces military-certified coaxial radio components.

(*Continued On The Following Column)

- **Limited Liability Company Uraldronzavod** is involved in computer programming activities and has developed a UAV used by the Russian MoD.
- **Limited Liability Company KB Rus** manufactures electronic components and has created a drone helicopter that is planned for use by Russia's military.
- **Limited Liability Company NPK Tesart** develops and manufactures technology, including radio-measurement systems, and its products are advertised on the website of U.S.-designated Scientific Equipment Group of Companies, a Russian company that provides high-tech equipment to industrial enterprises.
- **Limited Liability Company Company Scan** is a wholesaler of machinery and electronic equipment, including to the U.S.-designated Russian technology research institute Federal State Financed Institution of Science Physics and Technology Institute Named after A. F. Ioffe of the Russian Federation Academy of Sciences.
- **Limited Liability Company TC Element** is a wholesaler and technical services provider for machinery, computers, and analytical equipment, including spectrometers.
- **Limited Liability Company Vector** is a manufacturer of electronic components that imported millions of dollars' worth of high priority electronics, including electronic integrated circuits.
- **Nauchno Issledovatelskaya Laboratoriya Aerokosmicheskoi Tekhniki DOSAAF** (DOSAAF) has a research laboratory for aerospace technology, and manufactures radar equipment, radio navigation devices, and remote-control radio apparatuses. DOSAAF has also contributed to a project led by U.S.-designated Russian defense entity JSC Academic M.F. Reshetnev Information Satellite Systems.
- **Nauchno Proizvodstvennoe Predpriyatie Tomilinskii Elektronnyi Zavod** manufactures microchips allegedly used in missile production.
- **Nauchno Proizvodstvennoe Obyedinenie Gran** manufactures robots and other robotized vehicles used by Russian assault teams in Ukraine and for remote-controlled minelaying. **OJSC Vladimir Radio Communications Design Bureau** develops software and hardware systems, as well as radio communication systems for the Russian MoD.
- **Open Joint Stock Company MStator** produces high-tech electromagnetic components, including inductors for the Russian MoD.
- **Proteh Co Ltd** (Proteh) modernizes production facilities in the radio-electronic and instrument-making industries. Proteh works with U.S.-designated Russian defense conglomerate Rostec and has helped the U.S.-designated Russian UAV producer Special Technology Center acquire foreign-made components.
- Radioline Ltd (Radioline) designs, develops, and produces positioning systems for industrial robots. Radioline has also made agreements to procure technology for U.S.-designated Russian UAV producer Special Technology Center.

(*Continued On The Following Page)

- **Research and Production Association Lepton** manufactures remote sensing cameras and high-resolution telescope cameras that can provide military and intelligence collection capabilities.
- **Russian Artificial Intelligence Research Institute of the Russian Academy of Sciences** (RAIRI) develops systems related to artificial intelligence. A leading RAIRI researcher has presented on robotic systems at a Russian military forum.
- **Scientific and Production Association State Institute of Applied Optics**, a subsidiary of U.S.-designated Russian defense entity Joint Stock Company Shvabe, develops and produces advanced optoelectronic systems.
- **Scientific Production Association Computing Systems** manages IT infrastructure for the Russian MoD and the Russian Ministry of Internal Affairs.
- **Scientific Research Institute for Optoelectronic Instrument Engineering** (OIE) develops, creates, tests, and calibrates optoelectronic and laser devices. OIE has filed a patent related to defense technology.
- **Scientific Research Center Resonance Joint Stock Company** develops radar systems for the Russian MoD.
- **Speech Technology Center Limited** (STC) develops facial, voice, and biometric recognition software and systems. STC works with the FSB and Russian Ministry of Internal Affairs.
- STC Innovations Limited is an STC subsidiary that develops biometric and person-identifying technologies, including for government agencies.
- STC Soft Limited is an STC subsidiary that provides biometric search capabilities to Russian authorities.
- Sfera JSC (Sfera) develops software and facial recognition surveillance systems. The Russian Government has used Sfera surveillance systems to detain protestors.
- ZAO Svetlana EP develops microwave radiation-resistant semiconductor devices and technology for next-generation radar systems.

ANNEX 3: RUSSIA'S STRATEGIC METALS AND MINING SECTOR

The following Russia-based companies are involved in or provide services to Russia's metals industry.

Russian metals and mining companies

The following Russia-based companies were designated pursuant to E.O. 14024 for operating or having operated in the metals and mining sector of the Russian Federation economy.

- **Aktsionernoe Obshchestvo Evraz Kachkanarski Gorno Obogatitelny Kombinat** mines iron and metal ores and non-metallic minerals.
- **Aktsionernoe Obshchestvo Evraz Nizhnetagilski Metallurgicheski Kombinat** (NTMK) is one of the largest integrated steel production plants in Russia. NTMK's production and processing cycle includes coke production facilities, blast furnaces, steelmaking units, and seven rolling mills.
- Aktsionernoe Obshchestvo Evraz Obedinenny Zapadno Sibirski Metallurgicheski Kombinat is the largest steel producer in Siberia.
- Aktsionernoe Obshchestvo Evraz Vanadi Tula produces vanadium pentoxide that includes specific additive alloys for the manufacture of high-strength steel.

*(*Continued On The Following Column)*

- **Aktsionernoe Obshchestvo Obyedinennaya Ugolnaya Kompaniya Yuzhkuzbassugol** is a bituminous coal and lignite surface mining company.
- **AO Evraz Market** is a leading provider of steel for infrastructure projects, and a trading company involved in the supply of rebar, and flat, tubular, and rolled steel.
- **Limited Liability Company GRK Bystrinskoe** is an ore mining and processing plant.
- **Obshchestvo S OgranichennoI Otvetstvennostyu Raspadskaya Ugolnaya Kompaniya**'s activities include coal mining services, surface and underground coal mining, and the wholesale of coal, ores, and other minerals.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Shakhta Alardinskaya** develops coal mining sites and prepares, cleans, washes, screens, and sizes coal.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Shakhta Esaulskaya**'s activities include coal mining services and the wholesale of coal, ore, and other minerals.
- **Publichnoe Aktsionernoe Obshchestvo Raspadskaya** (Raspadskaya) specializes in the production and sale of coking coal.

Russian metals and mining support services companies

Russia-based **Aktsionernoe Obshchestvo Norilsk Avia** (Norilsk Avia) provides helicopter transportation services. Norilsk Avia was designated pursuant to E.O. 14024 for operating or having operated in the aerospace sector of the Russian Federation economy.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy:

- **Aktsionernoe Obshchestvo Norilski Gorno Metallurgicheski Kombinat Im AP Zavenyagina** is involved in holding company and securities management.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu AP Invest** (AP Invest) specializes in real estate transactions, particularly in secured lending and mortgage services. AP Invest has partnered with more than 20 banks.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Evrazkholding Finans** is engaged in financial intermediation, deposit banking, business credit, and financial transactions processing.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the transportation sector of the Russian Federation economy:

- **Aktsionernoe Obshchestvo Taimyrskaya Toplivnaya Kompaniya** is engaged in the retail, sale, wholesale, storage, and transshipment of chemical products.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Norilski Promyshlenny Transport** is engaged in freight transport services, including general and specialized freight trucking.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the technology sector of the Russian Federation economy:

*(*Continued On The Following Page)*

- **Limited Liability Company BaseAlt** is involved in custom computer programing services, software development, and the creation of operating systems. BaseAlt entered into a technology agreement with a Russian metals and mining conglomerate to develop and promote domestic digital products, including the development of an operating system with built-in information security tools.
- **Limited Liability Company Nornickel Sfera** is engaged in critical information infrastructure security and software product publishing.
- **Limited Liability Company Nornickel Sputnik** is involved in IT design and operational activities that support digital transformation efforts.
- **Serenity Cyber Security Limited Liability Company** (MTS Red) is involved in computer programming, computer consultancy, and information security. MTS Red and a Russian metals and mining conglomerate signed a 2024 cooperation agreement on information security for the development of cybersecurity products and services for the industrial sector.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the construction sector of the Russian Federation economy:

- **Limited Liability Company Nornikel Technical Services** constructs buildings, roads and highways, and engineering structures in Russia.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Pechengskoe Stroitelnoe Obedinenie** is involved in building construction and civil engineering works.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Vostokgeologiya** constructs, reconstructs, repairs, and maintains roads, railways, and road structures. It is also engaged in the construction, operation, and repair of limestone mining facilities.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu Zapolyarnaya Stroitelnaya Kompaniya** specializes in the construction and reconstruction of underground facilities and surface mine infrastructure.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the engineering sector of the Russian Federation economy:

- **Obshchestvo S Ogranichennoi Otvetstvennostyu Institut Gipronikel** provides general design services, customer engineering services, and field engineering services.
- **Obshchestvo S Ogranichennoi Otvetstvennostyu NN** conducts engineering surveys and engineering and technical design and provides construction project management, construction control and supervision, and technical advice.

The following Russia-based entities were designated pursuant to E.O. 14024 for operating or having operated in the manufacturing sector of the Russian Federation economy:

- **Obshchestvo S Ogranichennoi Otvetstvennostyu Norilski Obespechivayushchi Kompleks** manufactures metal structures and provides spare sparts and other equipment and products to enterprises engaged in mining, processing, metallurgy, construction, and maintenance.

(*Continued On The Following Column)

- **Obshchestvo S Ogranichennoi Otvetstvennostyu Norilsknikelremont** provides repair and maintenance services for metallurgical and concentration plant equipment; mining equipment; automotive vehicles and rolling stock; self-propelled diesel equipment; and instrumentation and automation systems.

MMK

Russia-based **Publichnoe Aktsionernoe Obschestvo Magnitogorskiy Metallurgicheskiy Kombinat** (MMK) was designated pursuant to E.O. 14024 for operating or having operated in the metals and mining sector of the Russian Federation economy. MMK is the largest iron and steel works company in Russia and a leading steelmaker globally. OFAC previously designated MMK pursuant to E.O. 14024 for operating or having operated in the financial services sector of the Russian Federation economy.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the persons above that are in the United States or in the possession or control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked. All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person. Non-U.S. persons are also prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as from engaging in conduct that evades U.S. sanctions. OFAC's Economic Sanctions Enforcement Guidelines provide more information regarding OFAC's enforcement of U.S. sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation.

In addition, foreign financial institutions that conduct or facilitate significant transactions or provide any service involving Russia's military-industrial base run the risk of being sanctioned by OFAC. For additional guidance, please see the updated OFAC advisory, "Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base," as well as OFAC Frequently Asked Questions (FAQs) 1146-1157.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the SDN List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's FAQ 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

Any persons included on the SDN List pursuant to E.O. 14024 may be subject to additional export restrictions administered by the Department of Commerce, Bureau of Industry and Security (BIS).
For identifying information on the individuals and entities sanctioned today, click here.

MISSION STATEMENT:

Given the geopolitical state of affairs with China, Russia, and Crimea, the Occupied territories of UKRAINE, Donetsk and Luhansk Oblast, embargoed countries and other specific threatening end users and entities, located in the United States and around the globe;

Evolutions in Business and the companies we serve, armed with robust compliance to the Export Administration Regulations, will adhere to best practices to protect our revenue and yours, and ensure the national security interests of the United States.

NOTE: In accordance with Title 17 U.S.C. Section 107, this material is distributed without profit or payment for non-profit news reporting and educational purposes only.

Keep up to date with latest trade news at:

www.eib.com

Check out our latest podcast: EIB Export News Episode 23 - Hurdles in Export Compliance

https://www.buzzsprout.com/1592353/15650283