EIB World Trade Headlines

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

November 1, 2022 - Volume 14, Issue 17

Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme

The Defendants Obtained Military Technology from U.S. Companies, Smuggled Millions of Barrels of Oil and Laundered Tens of Millions of Dollars for Russian Oligarchs, Sanctioned Entities and the World's Largest Energy Conglomerate

A 12-count indictment was unsealed today in federal court in Brooklyn, New York charging five Russian nationals, Yury Orekhov, Artem Uss, Svetlana Kuzurgasheva, also known as "Lana Neumann," Timofey Telegin and Sergey Tulyakov with various charges related to a global procurement, smuggling and money laundering network. Also charged were Juan Fernando Serrano Ponce, also known as "Juanfe Serrano" and Juan Carlos Soto, who brokered illicit oil deals for Petroleos de Venezuela S.A. (PDVSA), the Venezuelan state-owned oil company, as part of the scheme. On October 17, 2022, Orekhov was arrested in Germany and Uss was arrested in Italy, both at the request of the United States, and will undergo extradition proceedings.

Breon Peace, United States Attorney for the Eastern District of New York, Michael J. Driscoll, Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI), Jonathan Carson, Special Agent-in-Charge, U.S. Department of Commerce's Office of Export Enforcement, New York Field Office, and Andrew Adams, Director, Task Force KleptoCapture announced the charges.

"As alleged, the defendants were criminal enablers for oligarchs, orchestrating a complex scheme to unlawfully obtain U.S. military technology and Venezuelan sanctioned oil through a myriad of transactions involving shell companies and cryptocurrency. Their efforts undermined security, economic stability and rule of law around the world," stated United States Attorney Peace. "We will continue to investigate, disrupt and prosecute those who fuel Russia's brutal war in Ukraine, evade sanctions and perpetuate the shadowy economy of transnational money laundering."

"Today we announce the dismantling of a sophisticated network consisting of at least five Russian nationals and two Venezuelan nationals, each of whom are directly linked to corrupt state-owned

*(*Continued On The Following Page)*

NEWSLETTER NOTES

enterprises, who knowingly sought to conceal the theft of U.S. military technology and profit off black market oil," said FBI Assistant Director-in-Charge Driscoll. "This network schemed to procure sophisticated technology in direct support of a floundering Russian Federation military industrial complex. While America's adversaries may seek innovative means to undermine the United States, they will continuously be met with the FBI's resolve through tirelessly uncovering and overcoming all threats to U.S. national security, no matter where they may seek safe haven.

"Complex criminal schemes like this require sustained coordination and collaboration between federal law enforcement and international partners. I'm proud of our team of dedicated law enforcement professionals for their teamwork and dedication to enforcing U.S. export controls," stated U.S. Department of Commerce Special Agent-in-Charge Carson. "We will continue to enforce the unprecedented export controls implemented in response to Russia's illegal war against Ukraine and the Office of Export Enforcement intends to pursue these violators wherever they may be worldwide."

"Webs of shell companies, cryptocurrency and an international network of fraudsters failed to shield Orekhov and his cronies from apprehension by U.S. law enforcement. Stamping out evasion of export controls on military technology is among the Task Force's highest priorities, and today's arrests reflects the power of those controls when enforced by a dedicated team of expert agents and devoted foreign partners," stated Task Force KleptoCapture Director Adams.

As alleged, Orekov has served as the part owner, Chief Executive Officer and Managing Director of Nord-Deutsche Industrieanlagenbau GmbH (NDA GmbH), a privately held industrial equipment and commodity trading company located in Hamburg, Germany. The other owner of NDA GmbH is Artem Uss, the son of the governor of Russia's Krasnoyarsk Krai region. Kuzurgasheva served as the Chief Executive Officer of one of the scheme's shell companies and worked for NDA GmbH under Orekhov. Using NDA GmbH as a front company, Orekhov and Kuzurgasheva sourced and purchased sensitive military and dual-use technologies from U.S. manufacturers, including advanced semiconductors and microprocessors used in fighter aircraft, missile systems, smart munitions, radar, satellites and other space-based military applications. These items were shipped to Russian end users, including sanctioned companies controlled by Telegin and Tulyakov, such as Radioavtomatika, Radioexport and Abtronics, that serviced Russia's defense sector. Some of the same electronic components obtained through the criminal scheme have been found in Russian weapons platforms seized on the battlefield in Ukraine.

*(*Continued On The Following Column)*

In 2019, Orekhov travelled to the United States to source parts used in the Russian-made Sukhoi fighter aircraft and the American-made F-22 Raptor stealth fighter aircraft. Orekhov and Uss also used NDA GmbH as a front to smuggle hundreds of millions of barrels of oil from Venezuela to Russian and Chinese purchasers, including a Russian aluminum company controlled by a sanctioned oligarch and the world's largest oil refining, gas and petrochemical conglomerate based in Beijing, People's Republic of China. Serrano Ponce and Soto brokered deals worth millions of dollars between PDVSA and NDA GmbH, which were routed through a complex group of shell companies and bank accounts to disguise the transactions. In one communication with Serrano Ponce, Orekhov openly admitted that he was acting on behalf of a sanctioned Russian oligarch, saying "He [the oligarch] is under sanctions as well. That's why we [are] acting from this company [NDA GmbH]. As fronting." The scheme also involved falsified shipping documents and supertankers that deactivated their GPS navigation systems to obscure the Venezuelan origin of their oil.

Payment for NDA GmbH's illicit activities was often consummated in U.S. dollars routed through U.S. financial institutions and correspondent bank accounts. To facilitate these transactions, Orekhov and his coconspirators used fictitious companies, falsified "Know Your Customer" documentation and bank accounts in high-risk jurisdictions, causing U.S. banks to process tens of millions of dollars in violation of U.S. sanctions and other criminal laws. In one conversation with Soto, Orekhov bragged that "there were no worries...this is the shittiest bank in the Emirates…they pay to everything." The scheme also utilized bulk cash drops with couriers in Russia and Latin America, as well as cryptocurrency transfers worth millions of dollars, to effectuate these transactions and launder the proceeds.

On March 30, 2022, Orekhov asked the defendant Uss, "Have you decided to leave Russia?" Uss joked in response, "[Y]ou want to be an international fugitive?"

On March 2, 2022, the Attorney General announced the launch of Task Force KleptoCapture, 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 allies and partners, in response to Russia's unprovoked military invasion of Ukraine. The task force will leverage all the Department's tools and authorities against efforts to evade or undermine the economic actions taken by the U.S. government in response to Russian military aggression.

If convicted, the defendants face a maximum of 30 years' imprisonment. The charges in the indictment are allegations, and the defendants are presumed innocent unless and until proven guilty.

The government's case is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorney Artie McConnell is in charge of the prosecution, with valuable assistance from Trial Attorney Scott A. Claffee of the National Security Division's Counterintelligence and Export Control Section, and Litigation Analyst Ben Richmond.

Assistant United States Attorney Madeline O'Connor of the Office's Asset Recovery Section is handling forfeiture matters. The Justice Department's Office of International Affairs is providing substantial assistance. The United States thanks German and Italian authorities for their valuable assistance.

The Defendants:

YURY OREKHOV
Age: 42
Dubai, United Arab Emirates

ARTEM USS
Age: 40
Moscow, Russia

SVETLANA KUZURGASHEVA
Age: 32
Moscow, Russia

JUAN FERNANDO SERRANO PONCE
AGE: 47
Dubai, United Arab Emirates

JUAN CARLOS SOTO

TIMOFEY TELEGIN
Age: 39
Moscow, Russia

SERGEY TULYAKOV
Age: 52
Moscow, Russia

E.D.N.Y. Docket No. 22-CR-434 (EK)

The Impact of Sanctions and Export Controls on the Russian Federation

FACT SHEET
OFFICE OF THE SPOKESPERSON
OCTOBER 20, 2022

Since Russia launched its unjustified and unprovoked all-out war against Ukraine in February 2022, the United States has worked with Allies and partners around the world to impose an unprecedented range of sanctions and export controls on Russia for its brutal aggression. Moreover, we will continue to impose costs on the Kremlin for as long as its war of aggression continues. Sanctions and export controls are having significant and long-lasting consequences on Russia's defense industrial base. Since February 2022, the United States and our partners and Allies have coordinated to use export controls and sanctions to restrict Russia's access to advanced technology, which has degraded the Russian weapons industry's ability to produce and stockpile weapons to replace those that have been destroyed in the war.

A few effects include:

Major supply shortages for Russian forces in Ukraine are forcing Russia to turn to less technologically advanced countries such as Iran and North Korea for supplies and equipment.

Russia is struggling to import semiconductors and other key components. Export controls have forced Russia to cannibalize existing airline parts they can no longer access abroad.

Russian hypersonic ballistic missile production has nearly ceased due to the lack of necessary semiconductors used in the manufacturing process.

Russia's military aviation program has been cut off from resupply provided by global aviation trade.

Russian media reports that production of its next-generation airborne early warning and control military aircraft has stalled due to lack of foreign components, including semiconductors.

Mechanical plants, including those producing surface-to-air missiles, have been shut down due to shortages of foreign-origin components.

Russia has reverted to Soviet-era defense stocks because our measures have interrupted Russian companies' abilities to replenish domestic supply chains.

Exports on certain goods and services, including dollar-denominated banknotes, accounting, management consulting, quantum computing, and trust and corporate formation services to persons located in the Russian Federation are now prohibited.

*(*Continued On The Following Page)*

In addition, since February 2022, the U.S. government has:

Denied all [U.S.] exports, reexports to, and transfers of items subject to the Export Administration Regulations for military end uses or end users in the Russian Federation and Belarus.

Targeted Russian and Belarusian military end users through their addition to the Department of Commerce's Entity List, which has effectively cut off these end users from nearly all items subject to the Export Administration Regulations.

Denied exports to, reexports to, and transfer within Russia and Belarus of items needed for oil refining. Also imposed additional license requirements to further limit the Russian oil sector by restricting the export, reexport and transfer of additional items needed for oil refining.

Targeted items useful for Russia's chemical and biological weapons production capabilities and other advanced manufacturing by imposing export controls.

Targeted luxury goods to impose costs on certain Russian oligarchs who support the Russian government by imposing license requirements and denying licenses for the export and reexport of luxury goods for all end users within Russia.

Used new foreign direct product rules targeted at Russia to prevent exports of foreign-origin items produced with U.S. advanced technologies, tools, and software. This prevents these items being transferred to support Russia's military capabilities.

Formed a coalition of 37 countries that has amplified the impact of U.S. actions by applying substantially similar controls to those imposed by the United States. This robust global coalition reinforces U.S. efforts to isolate Russia from commodities, technologies, and software necessary for Putin's war.

Furthermore, sanctions (administered and enforced by the U.S. Department of Treasury) are having a significant impact on Russia's ability to wage its unjust war against Ukraine. Specifically, sanctions implemented by the United States along with Allies and partners and allies have immobilized about $300 billion worth of Russian Central Bank assets, limiting the central bank's ability to aid the war effort and mitigate sanctions impacts. Sanctioned Russian oligarchs and financial institutions have been forced to divest from long-held assets outside Russia. Moreover, sanctions have prompted banks in several countries to curtail ties with the Russian financial sector. Despite benefiting from high energy prices, the IMF still expects Russia's economy will contract by over 3 percent this year. Lost investment, export controls, and constraints on Russia's real economy will create a drag on Russia's growth prospects for years to come. Significantly, U.S. sanctions and export controls have severed Russia's access to key technologies and industrial inputs that erode its military capability.

*(*Continued On The Following Column)*

Since February 2022, the United States has issued approximately 1,500 new and 750 amended sanctions listings, including:

State Corporation Rostec, the cornerstone of Russia's defense-industrial base that includes more than 800 entities within the Russian military-industrial complex, such as Sukhoi, MiG, and Kalashnikov Concern.

Joint Stock Company Mikron, Russia's largest manufacturer and exporter of microelectronics.

Tactical Missiles Corporation JSC, a Russian state-owned enterprise that produces missiles used by the Russian Armed Forces in Ukraine.

Individuals and entities located outside Russia who have sought to procure goods and technology for the Russian military-industrial complex and intelligence services

Russia's largest financial institutions and restricted dealings with banks representing 80 percent of Russian banking sector assets.

Rosoboronexport, which is Russia's sole state-controlled intermediary agency for exporting and importing the entire range of military, defense, and dual-use products, technologies, and services.

Issued guidance emphasizing the sanctions and export control risk to individuals and entities inside and outside Russia that provide material support for Russia's sham referenda and purported annexation of the Kherson, Zaporizhzhya, Donetsk, and Luhansk regions of Ukraine.

****

Good afternoon,

My name is Mark Stephens and I'm an agency owner for an international non-asset carrier named Premier Expediters, Inc. (PEI). I've worked in transportation for over 30 years – the majority of which was spent as a dispatcher, driver, and in operations. After receiving my business degree, I combined the academia with my practical experience and started my own business as a freight broker. Shortly thereafter, I partnered with PEI to expand my network of services. I am a young business located in the White Mountains of New Hampshire and am working to expand my reach throughout New England and New York.

*(*Continued On The Following Page)*

PEI offers many traditional shipping needs (dry van, Conestoga, refrigerated, etc.), I specialize in open deck trailers - flatbed, step deck, RGN, lowboy, double drop, and more. I can ship to any destination you have, including the more difficult lanes some carriers avoid. As an organization, PEI has over 5000 vetted carriers in our database. The carriers we use go through a vetting process that ensures each company meets or exceeds the safety and insurance necessary to protect your freight and provide peace of mind. We take on that task so you can concentrate on other important aspects of your company.

In addition to the variety of equipment PEI offers, we can also be your specialized shipper for tradeshows, warehousing, date specific, oversized/out-of-gauge, and large projects. We maintain several noteworthy certifications to include SBA, CTPAT, Smartway, and WBENC. For more information on any of these certifications, please contact me and I will be happy to tell you about them.

As a new NHADE member, I would appreciate the opportunity to meet with you so I learn more about your logistical shipping needs and discuss how I can help you meet them in a reliable and fiscally responsible manner. Please pass along this email or my information to the correct person if needed. I would like to build my business by working with other businesses in the New England and New York area.

I have attached some additional information on PEI – Our MC# is 726137.

Thank you for your time and I look forward to talking with you soon

Mark Stephens
PEI ~ Premier Expediters, Inc.
Agency Owner ~ MC# 726137
Direct: (603) 545-9758
Email: mstephens@shippei.com
www.shippei.com

Commerce-Treasury-State Alert:

Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex[1]

Overview: Since Russia's unjustified and unprovoked invasion of Ukraine in February 2022, the United States has worked with allies and partners around the world to impose costs on Russia for its war of aggression. The Department of the Treasury's Ofice of Foreign Assets Control (OFAC), the Department of Commerce's Bureau of Industry and Security (BIS), and the Department of State are issuing this alert to inform the public of the impact of sanctions and export control restrictions targeting Russia's defense capabilities and warn of the risks of supporting Russia's military-industrial complex.

*(*Continued On The Following Column)*

Summary of actions taken in response to Russia's unjust war:
In response to Russia's attack on Ukraine, OFAC, BIS, and the Department of State, along with our foreign partners, have imposed an unprecedented range of sanctions and export controls.

Since February 2022, OFAC and the Department of State have:

Worked with partners and allies to immobilize about $300 billion worth of assets of the Central Bank of the Russian Federation, limiting the central bank's ability to aid the war effort and mitigate sanctions impacts.

Imposed sanctions on Russia's largest financial institutions and restricted dealings with banks representing 80% of Russian banking sector assets.

Issued approximately 1,500 new and 750 amended sanctions listings, including: State Corporation Rostec, the cornerstone of Russia's defense-industrial base that includes more than 800 entities within the Russian military-industrial complex, such as Sukhoi, MiG, and Kalashnikov Concern.

Joint Stock Company Mikron, Russia's largest manufacturer and exporter of microelectronics.

Tactical Missiles Corporation JSC, a Russian state-owned enterprise that produces missiles used by the Russian Armed Forces in Ukraine.

Numerous other defense-related firms determined to operate or have operated in the defense and related materiel, aerospace, electronics, marine, or technology sectors of the Russian Federation economy.
Non-Russian entities that have provided material support to Russian defense-procurement firms.

1 This alert is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive, or as imposing requirements under U.S. law, or otherwise addressing any requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

Determined eight sectors of the Russian Federation economy to be sectors in which persons who operate or have operated can be subject to sanctions, namely the financial services sector; the aerospace, electronics, and marine sectors; the accounting, trust and corporate formation services, and management consulting sectors; and the quantum computing sector of the Russian Federation economy.

These sector determinations complement pre-February 2022 sanctions administered by OFAC with respect to persons operating in the technology sector and the defense and related materiel sector of the Russian Federation economy.

Prohibited or implemented prohibitions on the exports on certain goods or services to persons located in the Russian Federation, including dollar-denominated banknotes; accounting, management consulting, and trust and corporate formation services; and quantum computing services.

*(*Continued On The Following Page)*

Issued guidance emphasizing the sanctions risk to individuals and companies inside and outside Russia that provide material support for Russia's sham referenda and purported annexation of the Kherson, Zaporizhzhya, Donetsk, and Luhansk regions of Ukraine.
Issued guidance emphasizing the sanctions risk to financial institutions that enter into new or expanded agreements with National Payment Card System Joint Stock Company (NSPK), the operator of Russia's Mir National Payment System.

Since February 2022, BIS has focused on degrading Russia's military capabilities and has:

Denied exports to, reexports to, and transfers within Russia and Belarus of items that are multilaterally controlled.
Denied exports to, reexports to, and transfers within Russia and Belarus of items on the Commerce Control List that are unilaterally controlled, including for anti-terrorism reasons.
Targeted military end users and put them on the Entity List. BIS is denying items to these end users, except in some very limited cases, such as for certain U.S. Government space collaboration involving the International Space Station.
Denied exports to, reexports to, and transfers within Russia and Belarus of a large subset of items that would otherwise be designated EAR99 (e.g., low-technology consumer goods not on the Commerce Control List). In most cases, we have identified these items by Harmonized Tarif
Schedule and Schedule B numbers.
Targeting oil refining. Denied exports to, reexports to, and transfer within Russia and Belarus of items needed for oil refining.

- Targeting various industrial and commercial items. Denied exports to, reexports to, and transfers within Russia and Belarus of a wide array of items needed by Russian industry, in order to further undermine the Russian defense industrial base.

- Targeting items useful for Russian's chemical and biological weapons production capabilities and other advanced manufacturing. Denied exports to, reexports to, and transfers within Russia and Belarus of items potentially useful for Russia's chemical and biological weapons production capabilities and items needed for advanced production and development capabilities, in order to hinder advanced manufacturing across a number of industries.
- Targeting "luxury goods" to impose costs on elites supporting Russian government. Denied exports, reexports, and in-country transfers of luxury goods for all end users within Russia or Belarus, and for certain Russian and Belarusian oligarchs and malign actors worldwide.

*(*Continued On The Following Column)*

Added foreign direct product rules (FDPRs) targeted at Russia and Belarus to be sure that

U.S. tools, sofware, and technology are not used to produce foreign items to support Russia's military capabilities.
Accordingly, BIS has imposed a FDPR to Russia and Belarus as destinations, and an even more expansive FDPR targeting Russian and Belarussian military end users.

Formed a coalition of 37 other countries, who have applied their own substantially similar controls. Because these countries are aligned with the United States, foreign produced items made in these countries are exempted from certain U.S. regulations.

Strategic Intent and Impact of Our Actions:

The strategic intent of our actions is to degrade Russia's ability to wage its unjust war against Ukraine and prevent Russia from projecting military force beyond its borders.

Sanctions and export controls are having significant and long-lasting consequences on Russia's defense industrial base, which relies extensively on foreign-sourced items. By restricting Russia's access to advanced goods, technology and services, the United States and our allies have degraded the Russian defense industry's ability to replace weapons destroyed in the war, including over 6,000 pieces of military equipment, such as tanks, armored personnel carriers, and infantry fighting vehicles.

For example, one of Russia's major tank producers, Uralvagonzavod, was reported to be due to a lack of foreign components and has had to furlough employees. Major supply shortages for Russian forces in Ukraine, in part because of sanctions and export controls, are forcing Russia to turn to less technologically advanced countries like Iran and North Korea for supplies and equipment.

Russia's defense industry is reliant on imported microelectronics. Since imposition of U.S. and allied restrictions, semiconductor imports from all global sources, the lifeblood of Russia's weaponry, have dropped on a sustained basis over time of approximately 70 percent. Russian hypersonic ballistic missile production has nearly ceased due to the lack of necessary semiconductors used

in the manufacturing process. The production of cars fell by three-quarters compared to last year, indicating that critical advanced microchips for civilian vehicles are being redirected for military use. The Russian military is reportedly cannibalizing chips from dishwashers and refrigerators to fix their military hardware, because they have run out of semiconductors. Russia's military aviation program no longer benefits from the revenue and resupply provided by aviation trade. Russian media reports that production of its next-generation airborne early warning and control (AEW&C) aircraf has stalled due to lack of foreign components, including semiconductors. Mechanical plants, including those producing surface-to-air missiles (SAMs), have been shut down. Russia has begun using Soviet-era defense stocks as its own companies are targeted by our measures.

*(*Continued On The Following Page)*

As flagged in recent guidance , OFAC is also prepared to use its broad targeting authorities against non-U.S. persons that provide ammunition or other support to the Russian Federation's military industrial complex, as well as private military companies (PMCs) or paramilitary groups participating in or otherwise supporting the Russian Federation's unlawful and unjustified attack on Ukraine. OFAC will continue to target Russia's eforts to resupply its weapons and sustain its war of aggression against Ukraine, including any foreign persons who assist the Russian Federation in those efforts.

Strategic Intent and Impact of Our Actions:

The strategic intent of our actions is to degrade Russia's ability to wage its unjust war against Ukraine and prevent Russia from projecting military force beyond its borders.

Sanctions and export controls are having significant and long-lasting consequences on Russia's defense industrial base, which relies extensively on foreign-sourced items. By restricting Russia's access to advanced goods, technology and services, the United States and our allies have degraded the Russian defense industry's ability to replace weapons destroyed in the war, including over 6,000pieces of military equipment, such as tanks, armored personnel carriers, and infantry fighting vehicles.

For example, one of Russia's major tank producers, Uralvagonzavod, was reported to be due to a lack of foreign components and has had to furlough employees. Major supply shortages for Russian forces in Ukraine, in part because of sanctions and export controls, are forcing Russia to turn to less technologically advanced countries like Iran and North Korea for supplies and equipment.

Russia's defense industry is reliant on imported microelectronics. Since imposition of U.S. and allied restrictions, semiconductor imports from all global sources, the lifeblood of Russia's weaponry, have dropped on a sustained basis over time of approximately 70 percent. Russian hypersonic ballistic missile production has nearly ceased due to the lack of necessary semiconductors used in the manufacturing process. The production of cars fell by three-quarters compared to last year, indicating that critical advanced microchips for civilian vehicles are being redirected for military use. The Russian military is reportedly cannibalizing chips from dishwashers and refrigerators to fix their military hardware, because they have run out of semiconductors. Russia's military aviation program no longer benefits from the revenue and resupply provided by aviation trade. Russian media reports that production of its next-generation airborne early warning and control (AEW&C) aircraf has stalled due to lack of foreign components, including semiconductors. Mechanical plants, including those producing surface-to-air missiles (SAMs), have been shut down. Russia has begun using Soviet-era defense stocks as its own companies are targeted by our measures.

*(*Continued On The Following Column)*

As flagged in recent guidance , OFAC is also prepared to use its broad targeting authorities against non-U.S. persons that provide ammunition or other support to the Russian Federation's military industrial complex, as well as private military companies (PMCs) or paramilitary groups participating in or otherwise supporting the Russian Federation's unlawful and unjustified attack on Ukraine. OFAC will continue to target Russia's eforts to resupply its weapons and sustain its war of aggression against Ukraine, including any foreign persons who assist the Russian Federation in those eforts.

While Russia has benefited from high energy prices and a store of foreign exchange reserves, the U.S.

Government has worked with partners and allies to immobilize about $300 billion worth of assets of the Central Bank of the Russian Federation, limiting the central bank's ability to aid the war efort and mitigate sanctions impacts. Sanctioned Russian oligarchs and financial institutions have been

forced to divest from long- held assets outside Russia. Sanctions on Russia's financial leadership have prompted banks in several countries to curtail ties with the Russian financial sector, for example by suspending use of Russia's Mir payment system.

From a macroeconomic perspective, Putin's war has resulted in a sharp economic contraction for Russia and will drag on Russia's economy for years to come. The International Monetary Fund (IMF), World Bank, and Organisation for Economic Co-operation and Development (OECD) forecasters expect Russia's economy to contract between 3.4 and 5.5 percent in 2022 and between 2.3 and 4.5 percent in 2023, roughly in line with private sector forecasts. Longer term, potential growth is expected to be very low, as Russia has shifed spending from investment to its military, lost access to key technologies, and diminished its human capital due to brain drain, while its companies have been severed from developed financial markets. Amid the impact of sanctions, Putin's choices, and the weak outlook, multinational corporations have fled Putin's Russia. According to estimates, over 1,000 global companies have curtailed or suspended operations in Russia. Academic and private sector analysts have estimated that that Russia's imports from the rest of the world fell around 30% in the wake of Russia's attack on Ukraine, and remain below levels observed prior to Putin's invasion.

Sanctions Evasion

To overcome the impacts on its military supply chain and to illicitly procure foreign technology, Russia is attempting to evade U.S. and partner sanctions and export controls using a range of techniques, including front companies and fraudulent end-user licenses.

*(*Continued On The Following Page)*

Existing sanctions authorities allow OFAC and the Department of State to impose sanctions on deceptive or structured transactions or dealings to circumvent any United States sanctions, as well as on persons that materially assist, sponsor, or provide financial, material, or technological support for, or goods or services to or in support of, sanctioned persons or sanctionable activities. OFAC and the Department of State have and will continue to use their authorities against persons inside and outside Russia that engage in sanctions evasion or circumvention.

For example, in March 2022, the Department of State designated a Russian defense-related firm, Radioavtomatika, due to its role as an entity specializing in the procurement of foreign items for Russia's military and defense industry. Since March, Radioavtomatika has attempted to leverage front companies and intermediaries in Uzbekistan, Armenia, and the People's Republic of China to continue its importation of critical technologies. In June 2022, the Department of State designated an Uzbekistan-based entity that actively supported Radioavtomatika in its eforts to evade U.S. sanctions. In September 2022, OFAC designated individuals, front companies, and foreign intermediaries associated with a Radioavtomatika procurement network set up to procure foreign items for Russia's defense industry. These designations should serve as a warning that those who support sanctioned Russian persons risk being sanctioned themselves.

Similarly, in June 2022, OFAC designated three Russian individuals and one entity based in Asia that were part of a covert procurement network linked to the Russian Federal Security Service (FSB). This FSB-linked network covertly procured U.S., Japanese, and European components for Russia's defense- industrial base through various foreign countries and bank accounts.

To assist industry identifying export control evasion, in June 2022 the Financial Crimes Enforcement Network (FinCEN) and BIS issued a joint alert that provides financial institutions with an overview of BIS's current export restrictions; a list of commodities of concern for possible export control evasion; and select transactional and behavioral red flags to assist financial institutions in identifying suspicious transactions relating to possible export control evasion.

Additional Information

For additional information about sanctions and export controls imposed in response to Russia's unjust war against Ukraine, please visit OFAC's website , BIS's website or State's page on Ukraine and Russia Sanctions.

Bread prices skyrocket as inflation grips Europe
Exports may be affected

VERDELOT, France — Since Russia's invasion of Ukraine, the price of the wheat that Julien Bourgeois grinds for boulangeries at his family's flour mill in central France has increased more than 30 percent. The bill for the electricity needed to run the mill has tripled. Even the price of paper used for flour sacks has hit the stratosphere.

U.K. Prime Minister Liz Truss announces resignation after 44 days in office and a tenure marked by economic and political turmoil

Truss could not regain support within her Conservative Party even after reversing her signature plan for big tax cuts for the wealthy and corporations, funded by big borrowing, which had spooked investors and sunk the British pound.

FOR IMMEDIATE RELEASE - Wednesday, October 19, 2022
European Nationals and Entities Indicted on Charges of Violating U.S. Laws for Their Attempt to Export a Dual-Use High-Precision Jig Grinder to Russia

A superseding indictment charging individuals and companies in Europe with violating United States export laws and regulations by attempting to smuggle a dual-use export-controlled item to Russia was unsealed yesterday in the District of Connecticut.

U.S. Attorney Vanessa Roberts Avery; Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division; Andrew Adams, Director of Task Force KleptoCapture; Special Agent in Charge Matthew B. Millhollin of Homeland Security Investigations (HSI), Boston; Special Agent in Charge Rashel D. Assouri of the U.S. Department of Commerce's Office of Export Enforcement, Boston; and Special Agent in Charge David Sundberg of the FBI New Haven Division made the announcement.

The indictment alleges that, beginning in 2018, Eriks Mamonovs, 33, and Vadims Ananics, 46, both citizens of Latvia who operated CNC Weld, a Latvia-based corporation, conspired with Stanislav Romanyuk, 37, a citizen of Ukraine and resident of Estonia who operated Estonia-based BY Trade OU, and others, including Janis Uzbalis, 46, of Latvia, and individuals in Russia and a Russia-based company, to violate U.S. export laws and regulations and smuggle a jig grinder that was manufactured in Connecticut to Russia. A jig grinder is a high-precision grinding machine system that does not require a license to export to European Union countries, but does require a license for export and reexport to Russia because of its potential application in nuclear proliferation and defense programs. At no time did the defendants apply for, receive or possess a license of authorization from the U.S. Department of Commerce to export or reexport the jig grinder to Russia, as required by the Export Control Reform Act of 2018 and the Export Administration Regulations ("EAR"), which restrict the export of items that could make a significant contribution to the military potential of other nations or that could be detrimental to U.S. foreign policy and national security.
U.S. authorities, working with Latvian authorities, intercepted the jig grinder in Riga, Latvia, before it was to be shipped to Russia.

Ananics, Mamonovs and Uzbalis were arrested yesterday in Riga, Latvia. Romanyuk was arrested in Tallinn, Estonia, on June 13. They are currently detained and the United States is seeking their extradition.

*(*Continued On The Following Page)*

"The power and precision of American technology must not be put to use by the Kremlin's war machine," said Andrew Adams, Director of Task Force KleptoCapture. "Enforcement against efforts to illegally export and reexport controlled U.S. technology is critical in ensuring that superior American technology isn't exploited by Russia in this unjust war. The arrests in Latvia extradition demonstrate that smugglers and fraudsters will be apprehended and prosecuted notwithstanding the sophistication of evasion networks operating far from U.S. shores."

"The indictment alleges that these defendants attempted to smuggle a high-precision export-controlled item to Russia where it could have been used in nuclear proliferation and Russian defense programs," said U.S. Attorney Vanessa Roberts Avery. "The danger created by such conduct is profound. I thank HSI, the Department of Commerce and the FBI, and our partners in Latvia and Estonia, who thwarted this alleged scheme and are working to bring these defendants to justice in a U.S. court of law."

"The power and precision of American technology must not be put to use by the Kremlin's war machine," said Andrew Adams, Director of Task Force KleptoCapture. "Enforcement against efforts to illegally export and reexport controlled U.S. technology is critical in ensuring that superior American technology isn't exploited by Russia in this unjust war. The arrests in Latvia demonstrate that smugglers and fraudsters will be apprehended and prosecuted notwithstanding the sophistication of evasion networks operating far from U.S. shores."

"These individuals are alleged to have conspired to export a piece of machinery that can be used for nefarious purposes, including in defense applications to build weapons of war," said Matthew Millhollin, Special Agent in Charge of Homeland Security Investigations in New England. "HSI works hand-in-hand with our partners domestically and abroad to further our mission to prevent sensitive U.S. technology and commodities from reaching the shores of hostile countries. These arrests and the seizure of the jig grinder are the result of the tenacious investigative work of our special agents and partners and show what can be achieved through these partnerships."

"This three-year investigation is a testament to the excellent cooperation between our domestic and international law enforcement partners," said Special Agent in Charge Rashel D. Assouri, U.S. Department of Commerce's Office of Export Enforcement, Boston Field Office. "The Office of Export Enforcement is unwavering in its aggressive pursuit to investigate illegal exports to Russia."

"This indictment is the culmination of a great collaborative law enforcement investigation," said David Sundberg, Special Agent in Charge of the FBI New Haven Division. "The alleged conspirators in this international export and money laundering scheme will now face justice in the very system they manipulated and violated for financial gain."

(*Continued On The Following Column)

The superseding indictment, which was returned by a federal grand jury in Hartford on July 7, 2022, charges Mamonovs, Ananics, Romanyuk, Uzbalis, and others, with conspiracy, an offense that carries a maximum term of imprisonment of five years; violation of the Export Control Reform Act, an offense that carries a maximum term of imprisonment of 20 years; smuggling goods from the United States, an offense that carries a maximum

term of imprisonment of 10 years; and international money laundering conspiracy, an offense that carries a maximum term of imprisonment of 20 years. Mamonovs is also charged with making false statements to the U.S. Department of Commerce, an offense that carries a maximum term of imprisonment of five years.

The indictment also charges CNC Weld, BY Trade OU with conspiracy, violation of the Export Control Reform Act, smuggling goods from the United States, and international money laundering conspiracy.

An indictment is merely an allegation, and each defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

This investigation is being conducted by HSI field offices in New Haven, Portland (Ore.), and the Hague, Netherlands; the U.S. Department of Commerce's Office of Export Enforcement in Boston; and the FBI. The Prosecutor-General's Office of the Republic of Latvia, the Prosecutor General's Office of the Republic of Estonia, Latvian Tax and Customs Police, Estonian Tax and Customs Board, and the Latvian State Police are assisting the investigation.

This case is being prosecuted by Assistant U.S. Attorneys Rahul Kale and Konstantin Lantsman of the District of Connecticut, and Trial Attorney Matthew Anzaldi of the Justice Department's National Security Division. The Justice Department's Office of International Affairs is providing valuable assistance.

The investigation was coordinated with the Justice Department's Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export controls, and economic countermeasures that the United States, along with its foreign allies and partners, has imposed in response to Russia's unprovoked military invasion of Ukraine. Announced by the Attorney General on March 2 and run out of the Office of the Deputy Attorney General, the task force will continue to leverage all of the Department's tools and authorities to combat efforts to evade or undermine the collective actions taken by the U.S. government in response to Russian military aggression.

Department of Justice U.S. Attorney's Office
District of New Hampshire - FOR IMMEDIATE RELEASE
Monday, October 17, 2022

Intertech Trading Corp. Sentenced to Pay $140,000 on 14 Felony Counts of Failure to File Export Information on Shipments of Lab Equipment to Russia and Ukraine

CONCORD – Intertech Trading Corporation, an Atkinson, New Hampshire-based laboratory equipment distributor, was sentenced today in federal court after pleading guilty to 14 felony counts of failure to file export information on shipments to Russia and Ukraine, United States Attorney Jane E. Young announced. Judge Paul Barbadoro ordered that Intertech pay the maximum allowable fine of $10,000 per count, for a total of $140,000, and be subject to a two-year term of corporate probation and monitoring.

According to court documents and statements made in court, between 2015 and 2019, Intertech exported laboratory equipment to Russia, Ukraine, and elsewhere, falsely describing the nature and value of the exported items on commercial invoices and shipping forms. In its plea agreement, Intertech admitted that it used false, innocuous descriptions such as "lamp for aquarium" or "spares for welding system," rather than accurately identifying the sophisticated scientific equipment actually contained in the shipments. Intertech admitted that it drastically undervalued the shipments, thereby evading the requirement to file Electronic Export Information, which would have been reported to the Departments of Commerce and Homeland Security.

"Evasion of export control requirements is a serious felony and undermines the government's ability to ensure that sensitive equipment does not end up in the wrong hands," said U.S. Attorney Young. "Our office works closely with our law enforcement partners to detect, deter, and punish companies and individuals that violate export control laws."

"Through lies and deceit, Intertech Trading Corporation evaded U.S. export laws to illegally send sophisticated scientific equipment to Russia and Ukraine, jeopardizing our national security," said Joseph R. Bonavolonta, Special Agent in Charge of the FBI Boston Division. "This case demonstrates how the FBI and our law enforcement partners will use all the resources at our disposal to ensure that sensitive technology doesn't end up in the wrong hands, and those who try and circumvent U.S. law will be held accountable."

This matter was investigated by the Federal Bureau of Investigation, Boston Division, and the Department of Commerce, Office of Export Enforcement. The case was prosecuted by Assistant U.S. Attorney Jarad Hodes and Trial Attorney David Lim of the National Security Division's Counterintelligence and Export Control Section.

Liz Truss to formally resign, Rishi Sunak to become U.K. Prime Minister. Follow our coverage.

Truss is scheduled to deliver farewell remarks outside Downing Street before submitting her resignation to King Charles III, ending her tenure as British prime minister after 49 days in office. Rishi Sunak, selected as the new leader by Conservative members of Parliament, will follow her to Buckingham Palace and ask the king for symbolic permission to form a government.

*(*Continued On The Following Column)*

Chinese officers charged in plot to obstruct US Huawei probe

By Eric Tucker and Nomaan Merchant | AP

October 25, 2022 at 6:57 a.m. EDT

WASHINGTON — Two suspected Chinese intelligence officers have been charged with attempting to obstruct a U.S. criminal investigation of Chinese tech giant Huawei by offering bribes to someone they thought could provide inside information, the Justice Department announced Monday.

The defendants are accused of paying tens of thousands of dollars in digital currency, along with cash and jewelry, to a U.S. official they thought they had recruited as an asset. But the person was actually a double agent working for the FBI, the department said.

Expanding U.S. Sanctions Authorities and Announcement of Visa Restrictions for Nicaraguan Officials

Press Statement
Antony J. Blinken, Secretary of State
October 24, 2022

Today, we are announcing steps to impose visa restrictions on over 500 Nicaraguan individuals and their family members. We are doing so pursuant to Presidential Proclamation 10309, which suspends entry into the United States as immigrants and nonimmigrants of members of the Government of Nicaragua and other persons who formulate, implement or benefit from policies or actions that undermine democratic institutions or impede the return to democracy in Nicaragua. These individuals include members of Nicaraguan security services, such as the Nicaraguan National Police, penitentiary officials, judges, prosecutors, higher education officials and non-government actors who enable regime repression and corruption as well as their family members. No member of the Nicaraguan government nor anyone who facilitates the Ortega-Murillo regime's abuses should believe they can travel freely to the United States.

The White House also announced an amendment to Executive Order (E.O.) 13851 on Nicaragua that expands sanctions authorities, including specific trade-related measures for Nicaragua. These new authorities will support our efforts to hold the Ortega-Murillo regime accountable. The regime's accelerating actions this year closing space for civil society, increasing its security cooperation with Russia, and silencing independent voices despite broad international calls for dialogue and moderation compel the United States to act. Governments that deny their people's basic rights or threaten the security interests of their neighbors should not expect that their political, economic, and trade relationships will remain unaffected.

*(*Continued On The Following Page)*

In conjunction with the E.O. announcement, the U.S. Department of the Treasury's Office of Foreign Assets Control imposed sanctions on Nicaraguan mining authority General Directorate of Mines, an office in the Ministry of Energy and Mines, and Reinaldo Gregorio Lenin Cerna Juarez, a close confidante of Nicaraguan President Ortega, pursuant to E.O. 13851.

The United States, together with our allies and partners, believes that a return to democracy and respect for human rights and fundamental freedoms in Nicaragua is essential. We will use diplomatic and economic tools available to promote accountability for the Ortega-Murillo regime, reiterate our call for the immediate and unconditional release of political prisoners, and urge the restoration of civic space for the people of Nicaragua.

For more information on today's action, see the White House and Treasury releases.

Simplifying the production of lithium-ion batteries

MIT spinout 24M Technologies designed a battery that reduces the cost of manufacturing lithium-ion cells.

Zach Winn | MIT News Office

Publication Date: October 25, 2022

When it comes to battery innovations, much attention gets paid to potential new chemistries and materials. Often overlooked is the importance of production processes for bringing down costs.

Now the MIT spinout 24M Technologies has simplified lithium-ion battery production with a new design that requires fewer materials and fewer steps to manufacture each cell. The company says the design, which it calls "SemiSolid" for its use of gooey electrodes, reduces production costs by up to 40 percent. The approach also improves the batteries' energy density, safety, and recyclability.

Judging by industry interest, 24M is onto something. Since coming out of stealth mode in 2015, 24M has licensed its technology to multinational companies including Volkswagen, Fujifilm, Lucas TVS, Axxiva, and Freyr. Those last three companies are planning to build gigafactories (factories with gigawatt-scale annual production capacity) based on 24M's technology in India, China, Norway, and the United States.

"The SemiSolid platform has been proven at the scale of hundreds of megawatts being produced for residential energy-storage systems. Now we want to prove it at the gigawatt scale," says 24M CEO Naoki Ota, whose team includes 24M co-founder, chief scientist, and MIT Professor Yet-Ming Chiang.

Establishing large-scale production lines is only the first phase of 24M's plan. Another key draw of its battery design is that it can work with different combinations of lithium-ion chemistries. That means 24M's partners can incorporate better-performing materials down the line without substantially changing manufacturing processes.

*(*Continued On The Following Column)*

The kind of quick, large-scale production of next-generation batteries that 24M hopes to enable could have a dramatic impact on battery adoption across society — from the cost and performance of electric cars to the ability of renewable energy to replace fossil fuels.

"This is a platform technology," Ota says. "We're not just a low-cost and high-reliability operator. That's what we are today, but we can also be competitive with next-generation chemistry. We can use any chemistry in the market without customers changing their supply chains. Other startups are trying to address that issue tomorrow, not today. Our tech can address the issue today and tomorrow."

A simplified design

Chiang, who is MIT's Kyocera Professor of Materials Science and Engineering, got his first glimpse into large-scale battery production after co-founding another battery company, A123 Systems, in 2001. As that company was preparing to go public in the late 2000s, Chiang began wondering if he could design a battery that would be easier to manufacture.

"I got this window into what battery manufacturing looked like, and what struck me was that even though we pulled it off, it was an incredibly complicated manufacturing process," Chiang says. "It derived from magnetic tape manufacturing that was adapted to batteries in the late 1980s."

In his lab at MIT, where he's been a professor since 1985, Chiang started from scratch with a new kind of device he called a "semi-solid flow battery" that pumps liquids carrying particle-based electrodes to and from tanks to store a charge.

In 2010, Chiang partnered with W. Craig Carter, who is MIT's POSCO Professor of Materials Science and Engineering, and the two professors supervised a student, Mihai Duduta '11, who explored flow batteries for his undergraduate thesis. Within a month, Duduta had developed a prototype in Chiang's lab, and 24M was born. (Duduta was the company's first hire.) But even as 24M worked with MIT's Technology Licensing Office (TLO) to commercialize research done in Chiang's lab, people in the company including Duduta began rethinking the flow battery concept. An internal cost analysis by Carter, who consulted for 24M for several years, ultimately lead the researchers to change directions.

That left the company with loads of the gooey slurry that made up the electrodes in their flow batteries. A few weeks after Carter's cost analysis, Duduta, then a senior research scientist at 24M, decided to start using the slurry to assemble batteries by hand, mixing the gooey electrodes directly into the electrolyte. The idea caught on.

The main components of batteries are the positive and negatively charged electrodes and the electrolyte material that allows ions to flow between them. Traditional lithium-ion batteries use solid electrodes separated from the electrolyte by layers of inert plastics and metals, which hold the electrodes in place.

*(*Continued On The Following Page)*

Stripping away the inert materials of traditional batteries and embracing the gooey electrode mix gives 24M's design a number of advantages.

For one, it eliminates the energy-intensive process of drying and solidifying the electrodes in traditional lithium-ion production. The company says it also reduces the need for more than 80 percent of the inactive materials in traditional batteries, including expensive ones like copper and aluminum. The design also requires no binder and features extra thick electrodes, improving the energy density of the batteries.

"When you start a company, the smart thing to do is to revisit all of your assumptions and ask what is the best way to accomplish your objectives, which in our case was simply-manufactured, low-cost batteries," Chiang says. "We decided our real value was in making a lithium-ion suspension that was electrochemically active from the beginning, with electrolyte in it, and you just use the electrolyte as the processing solvent."

In 2017, 24M participated in the MIT Industrial Liaison Program's STEX25 Startup Accelerator, in which Chiang and collaborators made critical industry connections that would help it secure early partnerships. 24M has also collaborated with MIT researchers on projects funded by the Department of Energy.

Enabling the battery revolution

Most of 24M's partners are eyeing the rapidly growing electric vehicle (EV) market for their batteries, and the founders believe their technology will accelerate EV adoption. (Battery costs make up 30 to 40 percent of the price of EVs, according to the Institute for Energy Research).

"Lithium-ion batteries have made huge improvements over the years, but even Elon Musk says we need some breakthrough technology," Ota says, referring to the CEO of EV firm Tesla. "To make EVs more common, we need a production cost breakthrough; we can't just rely on cost reduction through scaling because we already make a lot of batteries today."

24M is also working to prove out new battery chemistries that its partners could quickly incorporate into their gigafactories. In January of this year, 24M received a grant from the Department of Energy's ARPA-E program to develop and scale a high-energy-density battery that uses a lithium metal anode and semi-solid cathode for use in electric aviation.

That project is one of many around the world designed to validate new lithium-ion battery chemistries that could enable a long-sought battery revolution. As 24M continues to foster the creation of large scale, global production lines, the team believes it is well-positioned to turn lab innovations into ubiquitous, world-changing products.

*(*Continued On The Following Column)*

"This technology is a platform, and our vision is to be like Google's Android [operating system], where other people can build things on our platform," Ota says. "We want to do that but with hardware. That's why we're licensing the technology. Our partners can use the same production lines to get the benefits of new chemistries and approaches. This platform gives everyone more options."

Department of Justice U.S. Attorney's Office Western District of Texas

FOR IMMEDIATE RELEASE - Tuesday, October 25, 2022

Newly Unsealed Indictment Charges Ukrainian National with International Cybercrime Operation

Dedicated Website (Raccoon.IC3.gov) Announced to Assist in Identifying Malware Victims

AUSTIN – A newly unsealed federal grand jury indictment charges Mark Sokolovsky, 26, a Ukrainian national, for his alleged role in an international cybercrime operation known as Raccoon Infostealer, which infected millions of computers around the world with malware.

According to court documents, Sokolovsky, who is currently being held in the Netherlands pursuant to an extradition request by the United States, conspired to operate the Raccoon Infostealer as a malware-as-a-service or "MaaS." Individuals who deployed Raccoon Infostealer to steal data from victims leased access to the malware for approximately $200 per month, paid for by cryptocurrency. These individuals used various ruses, such as email phishing, to install the malware onto the computers of unsuspecting victims. Raccoon Infostealer then stole personal data from victim computers, including log-in credentials, financial information, and other personal records. Stolen information was used to commit crimes or was sold to others on cybercrime forums.

March 2022, concurrent with Sokolovsky's arrest by Dutch authorities, the FBI and law enforcement partners in Italy and the Netherlands dismantled the digital infrastructure supporting the Raccoon Infostealer, taking its then existing

Through various investigative steps, the FBI has collected data stolen from many computers that cyber criminals infected with Raccoon Infostealer. While an exact number has yet to be verified, FBI agents have identified more than 50 million unique credentials and forms of identification (email addresses, bank accounts, cryptocurrency addresses, credit card numbers, etc.) in the stolen data from what appears to be millions of potential victims around the world. The credentials appear to include over four million email addresses. The United States does not believe it is in possession of all the data stolen by Raccoon Infostealer and continues to investigate.

*(*Continued On The Following Page)*

The FBI has created a website where anyone can input their email address to determine whether it is contained within the U.S. government's repository of Raccoon Infostealer stolen data. The website is raccoon.ic3.gov. If the email address is within the data, the FBI will send an email to that address notifying the user. Potential victims are encouraged to fill out a detailed complaint and share any financial or other harm experienced from their information being stolen at FBI's Internet Crime Complaint Center (IC3) at ic3.gov/Home/FileComplaint.

"This case highlights the importance of the international cooperation that the Department of Justice and our partners use to dismantle modern cyber threats," said Deputy Attorney General Lisa O. Monaco. "As reflected in the number of potential victims and global breadth of this attack, cyber threats do not respect borders, which makes international cooperation all the more critical. I urge anyone who thinks they could be a victim to follow the FBI's guidance on how to report your potential exposure."

"I applaud the hard work of the agents and prosecutors involved in this case as well as our international partners for their efforts to disrupt the Raccoon Infostealer and gather the evidence necessary for indictment and notification to potential victims," U.S. Attorney Ashley C. Hoff said. "This type of malware feeds the cybercrime ecosystem, harvesting valuable information and allowing cyber criminals to steal from innocent Americans and citizens around the world. I urge the public to visit the FBI's Raccoon Infostealer website, find out if their email is within the stolen data, and file a victim complaint through the FBI's IC3 website."

"Today's case is a further reminder the FBI will relentlessly pursue and bring to justice cyber criminals who seek to steal from the American public," said FBI Deputy Director Paul Abbate. "We have once again leveraged our unique authorities, world-class capabilities, and enduring international partnerships to maximize impact against cyber threats. We will continue to use all available resources to disrupt these attacks and protect American citizens. If you believe you're a victim of this cybercrime, we urge you to visit raccoon.ic3.gov."

"This case highlights the FBI's unwavering commitment to work closely with our law enforcement and private sector partners around the world to hold cybercriminals accountable for their actions and protect the American people from cybercrime," said FBI Special Agent in Charge Oliver E. Rich Jr. "This case also serves as a reminder to public and private sector organizations of the importance to report internet crime and cyber threats to law enforcement as soon as possible. Working together is the only way we're going to stay ahead of rapidly changing cyber threats."

*(*Continued On The Following Page)*

"This indictment demonstrates the resolve and close cooperation of the Army Criminal Investigation Division and the FBI working jointly to protect and defend the United States," stated Special Agent in Charge Marc Martin, Army CID's Cyber Field Office. "Army CID would also like to thank our law enforcement partners in Italy and the Netherlands."

Sokolovsky is charged with one count of conspiracy to commit computer fraud and related activity in connection with computers; one count of conspiracy to commit wire fraud; one count of conspiracy to commit money laundering; and one count of aggravated identity theft. The Amsterdam District Court issued a decision on September 13, 2022, granting the defendant's extradition to the United States. Sokolovsky has appealed that decision.

If convicted, Sokolovsky faces a maximum penalty of 20 years in prison for the wire fraud and money laundering offenses, five years for the conspiracy to commit computer fraud charge, and a mandatory consecutive two-year term for the aggravated identity theft offense. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI's Austin Cyber Task Force, with the assistance of the Department of the Army Criminal Investigation Division (Army CID), is investigating the case. The FBI Austin Cyber Task Force is supported by Army CID, Austin Police Department, the Naval Criminal Investigative Service, the Round Rock Police Department and the Texas Department of Public Safety.

Victims of the Raccoon Infostealer can find more information at www.justice.gov/usao-wdtx/victim-assistance-raccoon-infostealer. Assistant U.S. Attorneys Michael C. Galdo and G. Karthik Srinivasan are prosecuting the case. The Department of Justice's Office of International Affairs is assisting with foreign evidence requests and the extradition request.

U.S. Attorney Hoff and Special Agent in Charge Rich would also like to thank the FBI Legal Attachés in Rome, The Hague, and Warsaw for their assistance in the investigation and disruption of the Raccoon Infostealer, along with the following foreign partners: Ministry of Justice of Italy; Special Unit for the Protection of Privacy and Technological Fraud of the Italian Guardia di Finanza; Procura della Repubblica di Brescia; the Netherlands Ministry of Justice and Security; Netherlands Police; and Netherlands Public Prosecution Service.

An indictment is merely an allegation and the defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

###

EXPORT CONTROLS IMPOSED ON ADVANCED COMPUTING AND SEMICONDUCTOR MANUFACTURING ITEMS TO THE PEOPLE'S REPUBLIC OF CHINA (PRC)

PUBLIC INFORMATION ON EXPORT CONTROLS IMPOSED ON ADVANCED COMPUTING AND SEMICONDUCTOR MANUFACTURING ITEMS TO THE PEOPLE'S REPUBLIC OF CHINA (PRC)

On October 7, 2022, the Bureau of Industry and Security (BIS) released a rule titled, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modifications" which implements new export controls.

This page provides useful information on that rule including links to the rule text, how the public can comment on the rule, and additional background information including Frequently Asked Questions (FAQs).

This page will be updated periodically as appropriate with additional information.
BIS Information on the Rule:

BIS's October 7, 2022 press release on the rule is available online here.

The written presentation of Assistant Secretary Thea D. Rozman Kendler for BIS's October 13, 2022 Public Briefing on the rule is available online here

A webcast of Under Secretary Alan F. Estevez's October 27, 2022 fireside chat at the Center for a New American Security (CNAS) discussing the rule is available online here.
Frequently Asked Questions (FAQs):

BIS's first round of FAQs, published on October 28, 2022 are available online here

Rule Text and Public Comment Information:
The text of the published rule on the Federal Register's website is available online here. To submit a public comment on the rule via Regulations.gov please follow this link.

https://www.bis.doc.gov/index.php/about-bis/newsroom/2082

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.

Evolutions in Business
Celebrating more than

30 Years