May 2023 | Vol. 37, No. 5

EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:

Challenges to Supply Chain Compliance

Forced Labor, Critical Minerals and Conflict Timber

WELCOME TO YOUR NEW

EXPORT PRACTITIONER™

IN PRINT | VIA EMAIL | ONLINE

VISIT ONLINE AT EXPORTPRAC.COM

FROM THE EDITOR:

After 37 years of delivering concise, timely information to the trade compliance community, The Export Practitioner has recommitted to its mission, with a new website. Enhanced graphics, richer citations, and a robust archival search, coupled with more timely updates empower readers, providing a "one-stop-shop" for export compliance professionals.

Disciplined reporting on BIS, DDTC, and OFAC ensures you are informed of the latest policy and regulatory developments, while a "Focus on Enforcement" furnishes memorable and illustrative cases to cite as you evangelize export compliance across the enterprise, from leadership to the rank and file.

We are broadening our subscriber offering, affording larger teams and entities the opportunity to share the resource, particularly in the academic and government community. Reach out to us to ensure your subscription gets to everyone who can use it.

Share your thinking with the Export Practitioner community

- We welcome original contributions from readers on all topics of interests to practitioners: Interpretation, education, and execution.
- Your submission will carry your byline. You'll get a link so you can share your story with clients and colleagues — even if they're not subscribers.

TO SUBSCRIBE, OR TO SUBMIT CONTENT:

Contact Editor Frank Ruffing at fruffing@traderegs.com, or call 301-460-3060.

EP
THE EXPORT PRACTITIONER™
MAY 2023 | VOL. 37, NO. 5

FEATURES

Supply Chain Compliance on the Rise

POLICY

EXPORT CONTROL

SANCTIONS

ENFORCEMENT

ON THE COVER: Cargo containers on a ship in port. KELLY / PEXELS

The Export Practitioner
www.exportprac.com

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

Published monthly by Gilston-Kalin Communications, LLC.

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

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

ISSN 1087-478K

FEATURE

The Rise of Supply Chain Compliance

As global supply chains become increasingly complex, businesses face significant challenges in ensuring compliance with laws, regulations, and industry standards. Non-compliance can lead to legal penalties, financial losses, and reputational damage, making supply chain compliance risk mitigation crucial.

Organizations are adopting innovative solutions, such as virtual supply chain centers of excellence (CoEs) and third-party managed services, to develop and implement comprehensive compliance programs. These programs focus on core issues such as visibility, transparency, communication, collaboration, and effective execution of compliance-related tasks.

The use of advanced analytics, improved visibility, and greater control over supply chain compliance enables companies to adapt to rapidly changing regulatory requirements and proactively monitor ongoing compliance.

Virtual supply chain CoEs provide a centralized, collaborative platform for sharing best practices, addressing risks, and ensuring compliance across the organization. Meanwhile, third-party managed services offer a cost-effective solution for resource-constrained organizations to implement process and technology improvements without significant capital investment.

Successful implementation of comprehensive compliance programs offers numerous benefits, including improved visibility into supply chains, better communication and collaboration within the organization, and minimized disruptions to normal business operations.

Companies are also focusing on specific supply chain risks such as product safety, security, technical regulations, labor and employment, and logistics and distribution. By adopting innovative solutions and designing scalable, flexible compliance programs that leverage advanced analytics, organizations can better adapt to rapidly changing supply chain environments, proactively monitor ongoing compliance, and mitigate risks associated with non-compliance in today's complex business landscape.

Slaves to Fashion: Chinese Firms Cited for Labor, Other Violations

CHINESE "FAST FASHION" PLATFORMS like Shein and Temu are expanding rapidly in the United States, raising concerns about exploitation of trade loopholes, sourcing relationships, product safety, and forced labor.

These companies, which rely on U.S. consumers using Chinese apps to curate and deliver products, have outpaced competitors like Zara and H&M, turning fast fashion into a $106.4 billion industry in 2022.

A report released by the US China Economic Security Review Commission details the concerns, highlighting the merchants' rapid growth, policy concerns, and reccomendations.

Labor, Legal and Environmental Concerns

Investigations in 2022 alleged that Shein failed to declare sourcing cotton from Xinjiang for its products, a violation of the Uyghur Forced Labor Prevention Act. Further reports suggest illegal labor conditions among suppliers of Chinese fast fashion firms and health hazards and environmental risks associated with Shein products.

Continues on next page

Continued from previous page

Additionally, Shein and other Chinese fast fashion firms have faced numerous copyright infringement accusations and lawsuits for intellectual property rights violations.

De Minimus Exemption

These companies present challenges to U.S. interests, including difficulties monitoring supply sources and ensuring fair market practices with U.S. competitors. They also exploit trade de minimis import exemptions, allowing them to avoid import duties on shipments to the United States valued below $800. As a result, Shein and similar firms have become a case study in Chinese e-commerce platforms outmaneuvering regulators to grow a dominant U.S. market presence. This practice costs the U.S. Department of the Treasury an estimated $10 billion a year in lost tariffs.

U.S. Market Share

Shein's market presence has grown significantly in the United States over the last three years. The company's aggressive digital and social media advertising campaigns, coupled with the expansion of online buying during the COVID-19 pandemic, led to Shein capturing 50% of all fast-fashion sales in the U.S. by November 2022. In May 2022, Shein's app briefly became the most downloaded app in the country, surpassing TikTok, Instagram, and Twitter.

Past Congressional Efforts on Chinese e-Commerce include Senators writing stern letters to the company seeking information on Shein's alleged sourcing of Xinjiang cotton. The COMPETE Act of 2022, sought to close the de minimis loophole, but was sidelined thanks to lobbying pressure from Amazon and the package delivery industry. Amazon's Marketplace is the largest single beneficiary of the de minimus exemption.

Last Fall, **CBP's John Leonard** reportedly got laughs and applause from an audience of importing officials with the joke: "China has a free-trade agreement with the U.S. — it's called de minimis.

Congress Questions Enforcement of Forced Labor Act

➤ The lead sponsors of the Uyghur Forced Labor Prevention Act (UFLPA), have written a letter to the Department of Homeland Security Under Secretary, Robert P. Silvers, expressing concerns about the transparency and effectiveness of the law's enforcement.

The legislation, which enjoys broad bipartisan support, aims to combat forced labor practices in China's Xinjiang Uyghur Autonomous Region (XUAR).

Chairs of the *Congressional-Executive Commission* on China **Rep. Christopher Smith** (R-NJ) and **Sen. Jeff Merkley** (D-OR) highlight issues with the applicability review process for detained goods, the limited number of entities on the Forced Labor Enforcement Task Force's Entity List, and challenges in addressing transshipment from third countries.

The letter calls for greater transparency and information regarding the law's implementation and expresses concerns about the release of detained goods without public or congressional reporting.

Additionally, the lawmakers ask for an expansion of the

Continues on next page

Continued from previous page

Forced Labor Enforcement Task Force (FLETF) Entity List, which identifies entities engaged in forced labor.

The bipartisan group acknowledged the challenges of enforcing the UFLPA amid global supply chains and **seeks to address issues of transshipment from third countries**. They request an update on the implementation strategy, tools, and resources needed to tackle this challenge effectively.

The lawmakers ask for information on the enforcement of UFLPA in relation to "de minimis" shipments from China, which allow vendors to send materials without reporting basic data if the value is under $800. The group cites concerns about Chinese companies such as SHEIN and TEMU using this loophole for direct-to-consumer purchases.

The Congressional-Executive Commission on China plans to hold a hearing with a panel of experts on trade, forced labor, and labor trafficking to further examine the UFLPA's implementation.

The group cites concerns about Chinese companies such as SHEIN and TEMU using the de minimus loophole for direct-to-consumer purchases.

OECD

Critical Minerals Export Restrictions on Rise

THE GLOBAL TRANSITION to a green economy faces a serious challenge as the supply of critical raw materials struggles to keep pace with growing demand, warns a new policy paper from the Organization for Economic Co-operation and Development (OECD).

The report, *Raw Materials for the Green Transition: Production, International Trade and Export Restrictions*, emphasizes the need for a substantial increase in production and international trade of these materials in order to meet net zero CO2 emissions targets.

Driven by the aftermath of the COVID-19 pandemic, trade tensions, and the ongoing impact of Russia's invasion of Ukraine, the prices of materials like aluminum and copper have soared to record highs. Although the production and trade of critical raw materials have expanded significantly in the last decade, this growth is insufficient to meet the projected demand for metals and minerals necessary for a global shift from fossil fuels to renewable energy technologies.

Among the materials with the largest production volume expansions are lithium, rare earth elements, chromium, arsenic, cobalt, titanium, selenium, and magnesium. However, these increases still fall short of the four- to six-fold rise in demand expected for the green transition. Meanwhile, global production of some critical raw materials, such as lead, natural graphite, zinc, precious metal ores and concentrates, and tin, has declined in the past decade.

OECD Secretary-General Mathias Cormann stated, "Policy makers must closely scrutinise how the concentration of production and trade coupled with the increasing use of export restrictions are affecting international markets for critical raw materials. We must ensure that materials shortfalls do not prevent us from meeting our climate change commitments."

Export Controls on the Rise

Concentration of production has become more pronounced, with China, Russia, Australia, South Africa, and Zimbabwe among the top producers and reserve holders. While the trade of critical raw materials remains relatively well diversified, there is increasing concentration of imports and exports amongst countries, which may lead to supply chain disruptions.

Since the OECD began collecting data in 2009, export restrictions on critical raw materials have seen a five-fold increase. Today, 10% of global exports in these materials face at least one export restriction measure.

China, India, Argentina, Russia, Viet Nam, and Kazakhstan have issued the most new export restrictions during this period and are also the countries with the highest shares of import dependencies for OECD nations.

The OECD warns that the trend toward increasing export restrictions could have significant effects on the availability and prices of critical raw materials, potentially jeopardizing the global green transition.

For more information on *Raw Materials Critical for the Green Transition: Production, International Trade and Export restrictions*, visit www.oecd.org/trade/topics/trade-in-raw-materials/.

FEATURE

Teak Logs, Irrawaddy River, Mandalay, Myanmar, 2011.

TERRY FEUERBORN (CC BY-NC 2.0)

Timber Traffic Working Group Announced

THE TIMBER INTERDICTION Membership Board and Enforcement Resource (TIMBER) Working Group, a new interagency collaboration, was announced at the TIMBER Trafficking Enforcement Roundtable April 19.

The event, held in Washington, DC, was part of the Earth Day celebrations and aimed to address the growing concerns related to illegal timber trafficking and its impact on climate change.

Principal Deputy Associate Attorney General Benjamin Mizer opened the event by emphasizing the Biden Administration's commitment to combating climate change and addressing environmental challenges, including the illegal trafficking of natural resources.

"The United States was the first country to address the issue of the trafficking of plant and plant products, including timber, in international commerce by amending the Lacey Act in 2008… These amendments gave law enforcement and prosecutors in the United States a powerful legal tool to deter and prosecute those who illegally commercialize plant and plant products. That includes timber — particularly timber taken in violation of foreign law and then smuggled into the United States."

The TIMBER Working Group's members include the Department of Justice, the Department of Agriculture, the Department of the Interior, and the Department of Homeland Security, as well as the U.S. Council on Transnational Organized Crime's Strategic Division.

Illegal logging is the third most lucrative form of transnational crime worldwide, after counterfeiting and illegal drug trafficking, and is valued at up to $152 billion USD annually. It has numerous negative effects, such as contributing to climate change, causing habitat and biodiversity loss, fostering other illicit activities, and funding terrorism and conflict.

The TIMBER Working Group aims to improve coordination and resources to combat timber trafficking by focusing on three main objectives: identifying and investigating complex timber trafficking cases domestically and internationally, developing new tools and techniques for prosecution, and building the capacity of partner governments to combat this illegal trade.

Assistant Attorney General Todd Kim, head of the Environment and Natural Resources Division (ENRD), highlighted the crucial role of ENRD in investigating and prosecuting timber trafficking offenses. The division has already secured the highest ever fine for timber trafficking in the Lumber Liquidators case and continues to actively pursue other investigations.

"I cannot discuss our ongoing matters," said Mr. Kim. "However, I can say that we continue to actively investigate and prosecute these cases. For example, this September we have a trial in Florida on a seven-count indictment for the alleged importation of wood products in violation of the Lacey Act, and other crimes. Other Lacey Act wood and wood-product investigations are ongoing."

Kim also stressed the importance of developing relationships with foreign governments and strengthening their ability to detect and prosecute timber trafficking offenses. In the coming months, ENRD will work directly with officials from Guatemala, Honduras, Cameroon, Indonesia, and Vietnam.

The TIMBER Working Group, through its interagency collaboration and coordination with foreign governments, is expected to significantly enhance the United States' efforts to combat illegal timber trafficking and its devastating environmental consequences.

Axelrod Clarifies Self Disclosure Policy

Disclosing results in reduced penalties; not disclosing risks increased penalties.

Assistant Secretary of Commerce for Export Enforcement Matt Axelrod issued an update to prior guidance on voluntary self-disclosure of possible violations of Export Administration Regulations (EAR) and disclosures about possible EAR violations by others.

The most significant change is that while self-disclosure continues to be considered a mitigating factor, the policy now clarifies that deliberate non-disclosure of significant violations will be considered an aggravating factor, increasing potential penalties.

Last June, a dual-track system for VSDs was implemented, resolving most minor infractions within 60 days. The policy update focuses on incentivizing submission of VSDs for significant violations. Since the change, BIS has not seen a material change up or down in the number of VSDs received.

Today's policy announcement is different from last June's. We specifically want to further incentivize the submission of VSDs when industry or academia uncovers significant possible violations of the EAR.

Note the modifier "significant" before "possible violations of the EAR." We're not focused on increasing the number of minor or technical VSDs we receive. In fact, we want to let VSD filers know that when they identify multiple minor technical violations close in time, they can submit one overarching submission (as opposed to in multiple separate VSDs) to help streamline the process on their end and conserve resources on ours.

Instead, we're interested in increasing the number of VSDs we receive that disclose significant possible violations - the types of violations that reflect potential national security harm.

Assistant Secretary of Commerce for Export Enforcement Matt Axelrod

To do that, we want everyone to understand the risk calculus. Under the existing BIS settlement guidelines, a VSD that is timely, comprehensive, and involves full cooperation substantially reduces the applicable civil penalty under the base penalty matrix. It may also entitle the filer to additional mitigation, including the possibility of a fully suspended penalty in certain cases.

Companies and universities should carefully consider the consequences of not disclosing significant possible violations. Disclosing results in reduced penalties, while not disclosing risks increased penalties. So, whatever the situation, a voluntary self-disclosure entitles the reporting entity to a steep and concrete reduction in potential monetary liability.

What we're clarifying, effective immediately, is how we apply the existing guidelines in situations where there is a deliberate non-disclosure of significant possible violations. When someone chooses to file a VSD, they get concrete benefits; when someone affirmatively chooses not to file a VSD,

Continues on next page

Continued from previous page

however, we want them to know that they risk incurring concrete costs.

Because this factor is a "General Factor," it is designed to be "either mitigating or aggravating." In the past, we have consistently applied it as a mitigating factor when a VSD has been filed after a potential violation was uncovered.

Going forward, we will also consistently apply this factor as an aggravating factor when a significant possible violation has been uncovered by a party's export compliance program but no VSD has been submitted.

In other words, when someone submits a VSD, they receive concrete and identifiable benefits under our guidelines. By the same token, however, when someone uncovers a significant possible violation but then affirmatively chooses not to file a VSD, they are running a substantial risk - because if it does come to our attention, the decision not to disclose will be considered an aggravating factor under our existing guidelines.

Encouraging strong compliance programs and compliance with rules also involves incentivizing reporting of potential EAR violations by others. Disclosing another party's possible violation can be considered a mitigating factor in future enforcement actions.

If a potential export control violation also involves sanctions violation, monetary rewards may be available through the Financial Crimes Enforcement Network (FinCEN) whistleblower program.

Treasury Releases DeFi Illicit Finance Risk Assessment

THE TREASURY HAS PUBLISHED the 2023 DeFi Illicit Finance Risk Assessment, the first illicit finance risk assessment conducted on decentralized finance (DeFi) in the world.

The assessment considers risks associated with what are commonly called DeFi services. While there is currently no generally accepted definition of DeFi, the term broadly refers to virtual asset protocols and services that purport to allow some form of automated peer-to-peer transactions, often through use of self-executing code known as "smart contracts" based on blockchain technology. This term is frequently used loosely by the private sector, often for services that are not functionally decentralized.

Actors like the Democratic People's Republic of Korea (DPRK), cybercriminals, ransomware attackers, thieves, and scammers are using DeFi services to transfer and launder their illicit proceeds. They are able to exploit vulnerabilities, including the fact that many DeFi services that have anti-money laundering and countering the financing of terrorism (AML/CFT) obligations fail to implement them.

"Risk assessments play a foundational role in promoting understanding of the illicit finance risk environment and more effectively protecting the integrity of the U.S. financial system," said, **Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.** "Our assessment finds that illicit actors, including criminals, scammers, and North Korean cyber actors are using DeFi services in the process of laundering illicit funds.

Capturing the potential benefits associated with DeFi services requires addressing these risks. The private sector should use the findings of this assessment to inform their own risk mitigation strategies and to take clear steps, in line with AML/CFT regulations and sanctions obligations, to prevent illicit actors from abusing DeFi services."

The primary vulnerability that illicit actors exploit stems from non-compliance by DeFi services with AML/CFT and sanctions obligations. DeFi services engaged in covered activity under the Bank Secrecy Act have AML/CFT obligations regardless of whether the services claim that they currently are or plan to be decentralized. Other vulnerabilities include the potential for some DeFi services to be out of scope for existing AML/CFT obligations, weak or non-existent AML/CFT controls for DeFi services in other jurisdictions, and poor cybersecurity controls by DeFi services, which enable the theft of funds.

While risk assessments are primarily designed to identify the scope of an issue, the study also includes recommendations for U.S. government actions to mitigate the illicit finance risks associated with DeFi services. These include:

- strengthening U.S. AML/CFT regulatory supervision
- considering additional guidance for the private sector on DeFi services' AML/CFT obligations
- assessing enhancement to address any AML/CFT regulatory gaps related to DeFi services.

The DeFi risk assessment builds upon Treasury's other recent national risk assessments and furthers the work outlined in Executive Order 14067 on "Ensuring Responsible Development of Digital Assets." It also includes a request for input from the private sector to inform next steps; Treasury welcomes feedback about the assessment.

FinCEN 2022 Year In Review Published

➤ The Financial Crimes Enforcement Network (FinCEN) has issued its FinCEN Year in Review for FY 2022.

The Year in Review is intended to help stakeholders gain insight into both FinCEN's efforts to support law enforcement and national security agencies, and how financial information — filed pursuant to the Bank Secrecy Act (BSA) — is used.

"The information that financial institutions provide to FinCEN is integral to promoting national security, and aiding law enforcement agencies in their efforts to investigate and prosecute criminals that abuse the financial system," said FinCEN Acting Director Himamauli Das. "We will continue to work with our partners to gather more information about how BSA reporting is being used, and the tangible outcomes that BSA reports make possible."

The Year in Review includes

• statistics from fiscal year 2022 on BSA reports filed;
• law enforcement queries of BSA data;
• requests made and information shared under Section 314 of the USA PATRIOT Act;
• information gained from FinCEN's FY22 Portal Query Performance Measure Survey;
• and information on FinCEN's various programs and regulatory actions. The document supports Section 6201 of the Anti-Money Laundering Act of 2020.

USTR Releases Special 301 Report on IP Protection

➤ The United States Trade Representative (USTR) has released the 2023 Special 301 Report on the adequacy and effectiveness of U.S. trading partners' intellectual property (IP) rights protection and enforcement. The annual report evaluates over 100 trading partners and highlights key concerns and improvements in IP protection.

Belarus was added to the Watch List due to its law that legalizes the unlicensed use of copyrighted works from certain foreign states. The country can also keep royalties from unlicensed usage, directly benefiting the Lukashenka regime.

Bulgaria was also added to the Watch List for not addressing deficiencies in online piracy investigations and prosecutions. The Special 301 review of Ukraine remains suspended due to Russia's invasion of the country.

Despite some positive developments in China, the country's pace of IP reform slowed, and concerns about technology transfer, trade secrets, and counterfeiting persist. The U.S. continues to monitor China's progress in implementing commitments under the United States-China Economic and Trade Agreement (Phase One Agreement).

Several trading partners, including Thailand, Vietnam, and Nigeria, have enacted major legal reforms to advance IP protection and enforcement. Others, such as Tunisia and Chile, have joined international IP treaties. However, the EU's promotion of exclusionary geographical indications (GI) policies remains a concern for the U.S.

The Report highlights ongoing issues related to online piracy and broadcast piracy, including stream-ripping, illicit streaming devices, and illegal IPTV services. The USTR also continues to engage with trading partners to address concerns on IP protection and enforcement, using bilateral engagement and other mechanisms.

In 2023, the U.S. has expanded and enhanced engagement with diverse and inclusive stakeholder groups to consider their perspectives on IP issues. For example, the U.S. organized workshops with stakeholders on the margins of the Asia-Pacific Economic Cooperation (APEC) meetings.

The Special 301 Report is an annual review of the global state of IP protection and enforcement, and this year placed 29 trading partners on the Priority Watch List or Watch List.

Seven countries on the Priority Watch List, including Argentina, Chile, China, India, Indonesia, Russia, and Venezuela, will be the focus of intense bilateral engagement in the coming year, according to the USTR.

EU

TTC Needs More Focus on Trade

➤ The United States and European Union need to produce more results on trade through the bilateral Trade and Technology Council, **European Trade Commissioner Valdis Dombrovskis** told an audience in Washington.

In particular, the global focus on dealing with climate change presents the opportunity to create "a green transatlantic marketplace," he told a program sponsored by the American Enterprise Institute.

The EU and United States should coordinate their climate policies in order to set standards for green products and avoid trade barriers, he said.

The TTC has produced results in the technology sphere, including coordinated sanctions and export controls on Russia for its invasion of Ukraine.

"But we need to deliver more on the trade side. I want to see clear trade deliverables," he stated. The EU official said he hopes to see movement on trade at the next TTC meeting at the end of May in Sweden.

As part of the green transition, Brussels and Washington are working on a targeted critical minerals agreement. Reaching the agreement is essential to ensuring the EU is treated fairly under the US Inflation Reduction Act's subsidies for electric vehicles.

Dombrovskis

The US critical minerals agreement with Japan has created a useful precedent to build on, according to Mr. Dombrovskis. He will be discussing the critical minerals agreement today with US Trade Representative Katherine Tai.

The EU's carbon border adjustment mechanism is nondiscriminatory and compliant with the World Trade Organization rules, but subsidies are not, he said.

The WTO and trade are essential to getting to net zero, Director-General Ngozi Okonjo-Iweala said at a program sponsored by the Washington International Trade Association last week.

The WTO can provide a forum for strategic cooperation on climate change, she said. The. agreement on fisheries subsidies reached last year at the 12th ministerial conference demonstrated that WTO members "can reach agreements for the global commons."

"Trade is a force for the rapid climate action that we need and nothing in the WTO rules prevents members from taking climate action," she stated.

Speaking at the same program, **Deputy Director General Angela Ellard** pointed out that the WTO has a full agenda of environmental issues, including fisheries subsidies, plastics pollution, fuel subsidies and structural sustainability.

She expressed hope that members might return to negotiations on an environmental goods agreement. Ms. Ellard, who previously was chief trade counsel for the House Ways and Means Committee, said there is increasing Congressional support for an EGA. WTO members, however, have not come to a decision on whether to resurrect the negotiations.

Assistant US Trade Representative for Environment and Natural Resources Kelly Milton said the WTO already has a full plate and should deal with the issues already on its agenda before turning to any new negotiations.

She suggested the WTO can be a platform for members to share and possibly coordinate their climate actions and to make sure that unintentional trade restraints are not being imposed.

COURTS

FSIA Does Not Protect Rogue State-Owned Actors

➤ The U.S. Supreme Court has rejected Turkey's state-owned Halkbank's claim that it is protected under the 1976 Foreign Sovereign Immunities Act (FSIA), which limits the jurisdiction of American courts over lawsuits against foreign countries. The court ruled that the FSIA does not provide foreign states and their instru-

Continues on next page

Continued from previous page

mentalities with immunity from criminal proceedings, according to conservative Justice Brett Kavanaugh.

Halkbank has been trying to avoid criminal charges in the United States for allegedly helping Iran evade American economic sanctions. The majority of the Supreme Court found that the 2nd Circuit did not fully consider whether the bank has immunity under "common law" principles.

In a dissenting opinion, Justice Neil Gorsuch argued that the FSIA does apply but that the bank's prosecution would still be allowed to proceed under the law's exceptions for commercial activity in or affecting the United States. He criticized the majority's decision for complicating the law unnecessarily and stated that lower courts lack guidance on resolving immunity disputes using common law.

President Joe Biden's administration maintained that the FSIA does not apply to criminal prosecutions and that Halkbank's actions fell under the law's exception to sovereign immunity for misconduct involving commercial activities. The U.S. government has been pursuing criminal matters against foreign government-owned companies for at least 70 years.

U.S. prosecutors accused Halkbank of converting oil revenue into gold and cash to benefit Iranian interests and documenting fake food shipments to justify transfers of oil proceeds. They also alleged

that Halkbank helped Iran secretly transfer $20 billion of restricted funds, with at least $1 billion laundered through the U.S. financial system.

The 2nd Circuit in 2021 ruled against Halkbank, concluding that even if the FSIA law shielded the bank, the conduct for which it was charged fell under the commercial-activity exception.

China Cloud Service US Prospects Dim

Huawei Cloud and Alibaba Cloud to Commerce's Entity List?

➤ Chinese cloud computing companies could pose a threat to US national security, Commerce Secretary Gina Raimondo told a Senate panel Wednesday.

She promised to review a request made by a group of Republican senators to add companies like Huawei Cloud and Alibaba Cloud to Commerce's Entity List, which would subject the firms to US export controls.

"I've put over 200 Chinese companies on the entity list in my tenure and we are actively, constantly investigating additional threats and if and as we think companies need to go onto the list, I will not hesitate," she said.

Ms. Raimondo appeared at the Senate Appropriations subcommittee hearing on the fiscal year 2024 budget request for Commerce. She noted that the request proposes an increase in funding for Commerce's Bureau of Industry and Security so that it can step up enforcement.

She was asked about security concerns surrounding the Chinese companies by Sen. Bill Hagerty (R-Tenn), who along with eight other Republican senators sent a letter to Administration officials urging that controls be imposed of Chinese cloud computing companies.

"We urge you to use all available tools to engage in decisive action against these firms, through sanctions, export restrictions, and investment bans, and to further investigate PRC cloud computing service companies," they wrote in a letter to Ms. Raimondo, Treasury Secretary Janet Yellen and Secretary of State Anthony Blinken.

In addition to Sen. Hagerty, the letter was signed by Republican Sens. Thom Tillis (NC), Marco Rubio (Fla), Steve Daines (Mont), Ted Cruz (Texas), Joni Ernst (Iowa), Katie Britt (Ala), Kevin Cramer (ND) and Dan Sullivan (Alaska).

Cuban Farming

U.S. Agro-Businesses Losing Patience with Slow Progress in Cuban Trade

➤ U.S. agro-businesses, participating in a trade tour in Cuba, expressed frustration over the slow progress in boosting commerce with Cuban farmers and called on the Biden administration to ease restrictions, allowing them to invest in the island's private agriculture sector.

Last May, President Joe Biden loosened restrictions on travel, remittances, and migration, promising the United States would do more to support Cuba's fledgling private sector. However, change has been too slow for the more than 100-member U.S. Agricultural Coalition for Cuba (USACC), which includes national and state farm organizations, corporations, and producers.

"We're losing, and we're tired of losing," said **USACC Chair Paul Johnson** during a gathering at a hotel in Havana, according to *Reuters*.

U.S. businesses are eager to sell their products to Cuba and invest in private sector farms and cooperatives, aiding their development. However, little has changed since a similar group of investors arrived last April. Many farms have closed due to lack of investment, equipment, fuel, and supplies, resulting in widespread food shortages across Cuba.

"It's frustrating to us in the United States because we believe it's something that we can fix. We need to go back to our government ... and insist that the private sector is a path forward to development," Johnson added.

Cuba, a long-time adversary of the United States, embraced socialism over capitalism after Fidel Castro's 1959 revolution. However, the communist-run government lifted a ban on private companies in August 2021, with over 7,000 such businesses opening since, according to an Economy Ministry list updated on March 23.

Investors from Mexico, Venezuela, Vietnam, China, Spain, and Russia, among others, have participated in state- and private business in Cuba. However, the United States remains an outlier. Last May, the U.S. Treasury Department authorized entrepreneur John Kavulich's company to invest in a small private business in Cuba's services sector — the first such approval in decades. Mr. Kavulich is president of the U.S.-Cuba Trade and Economic Council, an advocacy group.

Nevertheless, many similar requests are still pending, according to Johnson. "Obviously, that's just not good enough," he said. "We're capitalists. We invest in private business all around the world. Why can't we do it in Cuba?"

Despite some eased restrictions, the Cold War-era U.S. embargo on Cuba persists, prohibiting certain trade and financing between the two countries and complicating investment ties.

AUKUS Prompts Research Security Concerns, ITAR Changes

As tensions between the United States and China escalate, the AUKUS alliance — consisting of Australia, the United Kingdom, and the United States — has prompted research security concerns and changes to the International Traffic in Arms Regulations (ITAR).

These changes are designed to facilitate the AUKUS plan, announced in 2021, which aims to provide Australia with the technology and capability to deploy nuclear-powered submarines.

China has attempted to weaken Australia's alliance with the United States over the past several years by exploiting its position as Australia's leading trade partner and meddling in the Australian political system through its foreign interference campaign.

In response, the United States and Australia have strengthened their partnership through intelligence sharing under the Five Eyes network and increased cooperation in defense and security.

On July 19, 2022, the State Department's Directorate of Defense Trade Controls (DDTC) published Open General License (OGL) No. 1 and OGL No. 2, which authorize reexports to or retransfers within the U.K., Canada, and Australia of certain types of defense articles, services, and technical data controlled under ITAR.

Australian researchers have expressed concerns that these controls will continue to stifle communications, with one scientist stating, "It's explicitly stated that researchers would be prohibited by any means – e-mails, papers, or speeches – to a [foreign recipient]."

To address this issue, the Department of State is amending Supplement No. 1 to part 126 to expand the types of defense articles that may be exported and defense services that may be furnished.

• First, this final rule amends the 25th entry, identified as USML Category IV which previously excluded "[d]efense articles and services specific to torpedoes," to exclude only "defense articles and services specific to the warhead or the sonar, guidance, and control section of torpedoes."

• Second, this final rule amends the 105th entry, identified as USML Category XX(c), which previously excluded "[d]efense articles and services specific to submarine combat control systems," to remove mounting racks and cabinets from that entry.

• Third, this final rule amends the 60th entry, the 66th entry, and explanatory Note 9 to remove specific Underwater Acoustic Decoy Countermeasures (ADC) from Supplement No. 1 and clarify the note.

• Fourth, this final rule amends the 28th and 29th entries regarding USML Category IV(i) manufacturing

Continues on next page

HMS Westminster fires Harpoon anti-ship missiles

Continued from previous page

know-how and the 67th – 70th entries regarding USML Category XII night vision.

The changes to ITAR regulations are intended to enhance the operational capabilities, interoperability, and cooperation between the armed forces of the United States and its allies and partners.

The AUKUS plan, which has a quarter-trillion dollar budget, includes the production and operation of a new submarine class, SSN-AUKUS, in addition to sharing advanced technology such as artificial intelligence and hypersonic weapons. In a recent panel discussion, Stephen Lovegrove, Britain's former national security adviser, acknowledged that Britain had fallen behind in hypersonic technology and expressed optimism that the AUKUS partnership would help bridge the gap.

Eric Schmidt, an adviser to the United States Department of Defense on artificial intelligence, emphasized that China's focus on drones, hypersonic, and automation technology should inform Australia's military spending decisions. While Schmidt acknowledged that a technological decoupling between China and Western allies is likely, he maintained that China is not an enemy and collaboration in other areas remains possible.

Michelle Simmons, Australia's leading quantum computer scientist, highlighted the challenges AUKUS will face, such as foreign investment and visa restrictions, in fostering collaboration. Simmons called for a "joint mission" among the three nations to develop a quantum computer, stressing the importance of pooling resources to maintain a competitive edge.

As the AUKUS alliance moves forward with its ambitious plans, it must navigate the complex landscape of research security concerns and regulatory changes to ensure the continued strengthening of defense and security ties among its member nations.

G7 Trade Ministers Target China's Economic Practices

➤ Trade ministers from the Group of Seven (G7) nations convened in a virtual meeting hosted by Japan, this year's G7 president, to discuss concerns about global economic issues, including "economic coercion" and non-market trade practices. These issues are believed to be aimed at China, whose trade policies have increasingly come under scrutiny.

The ministers also highlighted the need for major reforms within the World Trade Organization (WTO) and released a joint statement outlining their commitment to maintain and strengthen the global trading system. They acknowledged the disruptions caused by the ongoing conflict in Ukraine and the COVID-19 pandemic, but also emphasized the underlying developments in international trade, including non-market policies and practices.

The G7 ministers agreed to work towards reforming all three functions of the WTO, with the goal of having a fully functional dispute settlement system accessible to all members by 2024. They also expressed their shared concerns about non-market policies and practices, pledging to pursue more effective use of existing tools and develop new ones to address these challenges.

The joint statement also underscored the importance of supply chain resilience and security, expressing serious concern about economic coercion that interferes with the legitimate choices of other governments. The ministers committed to using their existing tools and developing new ones to deter and counter the use of coercive economic measures.

Moreover, the G7 ministers reaffirmed their commitment to export controls as a fundamental policy tool to address technology diversion, national security threats, and other challenges. They emphasized the importance of cooperation on export controls related to critical and emerging technologies, such as microelectronics and cyber surveillance systems.

The ministers also acknowledged the need to deepen discussions on business and human rights and accelerate the exchange of information on relevant regulations and policies. In addition, they pledged to continue working collaboratively on environmental and digital trade issues.

The G7 trade ministers will reconvene in October to further address these concerns and instruct their officials to accelerate work in preparation for the meeting.

Blue Lantern End Use Monitoring Report

THE BLUE LANTERN PROGRAM, managed by the Country and End-Use Analysis Division (CEA) of the Department of State, is designed to ensure the security and integrity of U.S. defense trade. The program is designed to minimize the risk of diversion and unauthorized use of U.S. defense articles, combat gray arms trafficking, uncover violations of the AECA, and build confidence and cooperation among defense trade partners.

It monitors the end-use of defense articles (including technical data), defense services, and brokering activities under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). Several Blue Lantern checks not only reviewed specific transactions but also analyzed the management structure and security controls of foreign companies that may pose a risk of diversion due to their acquisition by another foreign entity.

Program Activities: In FY 2022, CEA initiated 305 Blue Lantern checks in over 60 countries. The program included pre-license, post-license/pre-shipment, and post-shipment checks. The Blue Lantern program was affected by Russia's invasion of Ukraine in February 2022, leading to a suspension of routine checks and a reliance on consultations with the Ukrainian Embassy in Washington, DC, for transaction verifications. In-country end-use checks in Ukraine resumed in FY 2023 with limited site visits, as security conditions allow, and will be counted as part of the report for the next fiscal year.

Results: Of the 226 Blue Lantern checks closed in FY 2022, 159 (70%) reported "favorable" results, while 67 (30%) were deemed "unfavorable." Unfavorable checks were due to inconsistencies in the license application, unresponsiveness of a foreign party, or discrepancies in the information provided by the foreign party. **No instances of potential or actual diversion were documented, but three instances of unauthorized reexports/retransfers were identified.**

Actions Taken: Unfavorable Blue Lantern cases led to various actions, including denying or returning license applications without action, removing parties from licenses, updating the DDTC Watch List, or referring cases to the Office of Defense Trade Controls Compliance (DTCC) and/or U.S. law enforcement agencies for investigation and action. **Seven unfavorable checks were referred to DTCC in FY 2022.**

Regional Distribution of Unfavorable Cases: The NEA (North Africa & Middle East) region had the highest percentage of unfavorable checks (33%), primarily due to derogatory information on foreign parties. The EUR (Eurasian) and EAP (East Asian & Pacific) regions had unfavorable rates of around 30%, while the AF (Aftica) and SCA (South Central Asia) regions had unfavorable rates of 40% and 50%, respectively. There were no unfavorable checks in the WHA (Western Hemisphere) region in FY 2022.

Firearms Cases: Of the 226 Blue Lantern checks closed in FY 2022, 36 involved U.S. Munitions List (USML) Category I (Firearms), with three of these cases being deemed unfavorable. The unfavorable rate for checks involving USML Category I articles was 8% for FY 2022.

DDTC Watch List: In FY 2022, CEA reviewed 65,677 DDTC Watch List name matches and made 1,536 new entries and 2,096 modifications to the list. The Watch List is an internal screening tool containing over 229,000 entities and is used to flag export authorization applications for possible Blue Lantern checks. Since FY 2020, CEA has shared the DDTC Watch List with the Department of Commerce's Bureau of Industry and Security to improve its ability to regulate items under its control.

EXPORT CONTROL

Bio Research Export Rule Advances

➤ The Bureau of Industry and Security (BIS) is soliciting further comment on control measures for automated peptide synthesizers. Peptides and polypeptides are chains of amino acids, and proteins are composed of one or more large chains of polypeptides.

The proposed rule intends to control emerging and foundational technologies identified as essential to U.S. national security. The rule would apply to all persons engaged in the export, reexport, or transfer of automated peptide synthesizers and related technology. The proposal would primarily impact research and development activities in the biotechnology field. These items will retain reasons for control relating to the proliferation of chemical and biological weapons and anti-terrorism.

On September 13, 2022, BIS published an Advance Notice of Proposed Rulemaking (ANPRM) on the imposition of Section 1758 Technology Export Controls on Instruments for the Automated Chemical Synthesis of Peptides. BIS received five comments in response:

• One commenter argued that automated peptide synthesis is not viable for producing toxins, except for conotoxins. BIS agreed that the current instrumentation is limited, but believes it can still produce enough peptide toxin to cause mortality and morbidity within a population.

• Another commenter stated that controlled toxins can be produced manually and suggested export controls for reagents and consumables. BIS acknowledged the comments and will investigate potential export controls for peptide synthesis consumables.

• One commenter emphasized the benefits of new technological developments in peptide synthesizers for drug candidate research. BIS agreed with the usefulness of these technologies, but noted that they could also be used for dangerous purposes, such as in weapons programs.

• Several commenters suggested that BIS should not unilaterally control these technologies, as it could impact U.S. technology leadership in the field. BIS will work with international partners to provide multilateral controls but may take unilateral action if necessary.

• A commenter noted that most large-scale peptide production occurs manually. While BIS acknowledged this, they still intend to propose regulatory text for automated peptide synthesizers.

The proposed regulatory changes will add a new item paragraph (.k) with three subparagraphs (.k.1, .k.2, and .k.3) to ECCN 2B352. This paragraph will control peptide synthesizers that are partly or entirely automated, capable of generating continuous peptide sequences greater than 75 amino acids, and capable of producing 100 mg of peptide at 75% or greater purity in a single run.

BIS estimates that it will receive 40 license applications per year for the items described in this proposed rule.

BRIEFS

STATE

ITAR / USML Revision on Technological Progress

➤ The US Department of State is removing certain **high-energy storage capacitors** from the U.S. Munitions List (USML) as they are widely available internationally and do not provide a critical military or intelligence advantage.

The Department is also adding a 125-volt voltage criterion for the high-energy capacitors that remain on the USML. This is because certain low-voltage high-energy storage capacitor technology has progressed, and many models that exceed the existing USML control criteria no longer provide a critical military or intelligence advantage.

These lower-voltage capacitors are well understood, have been extensively integrated into commercial applications, and are widely available internationally without multilateral export restrictions.

Effective date of amendment is May 21, 2023. Send comments by May 30, 2023. [88 FR 25488]

Section 655 Report on Foreign Defense Sales

➤ The State Department has released its annual report to Congress on direct commercial sales authorizations for fiscal year 2022. The report, required by Section 655 of the Foreign Assistance Act of 1961, as amended, documents defense articles and services licensed for permanent export under Section 38 of the Arms Export Control Act (AECA), 22 U.S.C. 2778.

The report provides information on defense articles and services authorized for each foreign country and international organization during the fiscal year, along with data on actual shipments of those licensed transactions. The report notes that International Military Education and Training activities will be reported separately.

The full report can be accessed on the DDTC website.

Mission to Cajole Porous Border States

Treasury and Commerce meet to staunch materiel flow

Top Treasury Department officials took a two-week journey through Central Europe and Central Asia to garner support for measures countering Russia's evasion of sanctions imposed due to the ongoing war in Ukraine.

Brian Nelson, Under Secretary of the Treasury for Terrorism and Financial Intelligence, visited Central Europe, while **Elizabeth Rosenberg, Assistant Secretary for Terrorist Financing and Financial Crimes**, headed to Central Asia.

The two officials used their trips to foster closer collaboration, information sharing, and discussions on trade trends and enforcement priorities throughout the supply chain.

The Treasury Department notes that Russia is actively attempting to bypass sanctions imposed by a coalition of more than 30 countries.

In partnership with the Commerce Department and other US government departments and agencies, as well as international coalition partners, the Treasury Department is presenting businesses with a clear choice: maintain connections to the global economy or support Russia's war and lose access to the world's most crucial markets.

During his Central Europe visit, Mr. Nelson met with government officials, financial institutions, businesses with exposure to Russia, and key industry stakeholders. Addressing a group of business leaders at the American Chamber of Commerce Austria Roundtable, Mr. Nelson highlighted the success of the sanctions and export controls.

He assured the audience that business considerations were taken into the sanctions regime. Collaboration between the private sector and government authorities was encouraged, " We need to hear from you about what your firms are seeing in this space, and how you are managing the overlapping sanctions evasion risks, money laundering and fraud risks, and export controls requirements," he said.

Almaty

Mr. Nelson acknowledged concerns about the impact of sanctions on profits: "While we support increased scrutiny, we also want to ensure that jurisdictions are not subject to unnecessary de-risking, which

Continues on next page

Continued from previous page

could have significant unintended economic and financial consequences, especially in smaller jurisdictions."

Meanwhile, in Central Asia, Assistant Secretary for Terrorist Financing and Financial Crimes Elizabeth Rosenberg travelled with counterparts from the European Union, the United Kingdom, and the Commerce Department, to Kazakhstan to discuss the evasion of sanctions and export controls imposed on Russia for its war against Ukraine.

Ms. Rosenberg and Assistant Secretary for Export Enforcement Matthew Axelrod joined an interagency, multilateral visit to Astana and Almaty from April 23 to 26. They were part of a delegation that included the European Union's International Special Envoy for the Implementation of EU Sanctions, David O'Sullivan, and the United Kingdom's Director of the Sanctions Directorate, David Reed.

The delegations met with government officials and the private sector to share information, outline strategic priorities, and offer assistance to help facilitate compliance while minimizing economic impacts on Kazakhstan.

Russia's efforts to illicitly procure supplies and inputs for its military-industrial complex were discussed, with a focus on dual-use goods. The delegations urged vigilance against an uptick in evasion attempts and warned that Russia has sought to use cut-outs, opaque payments, and third countries to circumvent sanctions and export controls.

Assistant Secretary Axelrod stressed the urgency of preventing Russia from evading coalition export restrictions by transshipping specific semiconductors and other electronic integrated circuits through Kazakhstan to power its missiles and drones.

Assistant Secretary Rosenberg outlined sanctions evasion typologies in the financial sector and shared that the United States enjoys strong partnership and open communication with the Government of Kazakhstan. Both officials expressed the desire to be good partners to government and industry in their efforts to ensure they are not used to support the Russian war effort.

The visit aimed to provide clarity across sanctions and export control regimes and offer technical assistance to Kazakhstan.

Report: China Transshipments of U.S. Chips to Russia Up

➤ Despite US sanctions on Russia following the invasion of Ukraine, hundreds of millions of dollars' worth of US-made semiconductors continue to flow into Russia through circuitous routes, according to reporting in Nikkei Asia. A large portion of these chips are channeled through small traders in Hong Kong and mainland China.

Records from February 24 to December 31, 2022, showed 2,358 transactions, totaling at least $740 million, labeled as products of US chipmakers such as Intel, AMD, and Texas Instruments. About 75% of these transactions were shipped from Hong Kong or mainland China, amounting to $570 million.

The value of these exports increased tenfold compared to the same period in 2021. High-performance chips sought by Russia are used to control missiles and defense systems. The export data includes microprocessors from Intel and AMD, FPGAs from Xilinx (an AMD subsidiary), chips from Analog Devices, Texas Instruments, and On Semiconductor, and high-end radio frequency chip components from Qorvo.

Major chipmakers like Intel, Texas Instruments, Analog Devices, and On Semiconductor have stated that they do not sell to Russia or other sanctioned countries and are in compliance with all applicable laws and regulations, including US export controls. Analog Devices assets they have been putting extra effort into combating unauthorized resales but acknowledged the extreme difficulty of stopping such shipments entirely.

Although chipmakers and established distributors face close scrutiny from US authorities, numerous smaller traders, including one-person operations and recently established businesses, are harder to monitor. These small, lesser-known chip distributors may not follow "know your client" principles strictly.

Enforcing sanctions and cracking down on secondary chip sales to Russia or other sanctioned parties is challenging, as small trading companies can easily change names or operate under new names even if subjected to sanctions. The globalized supply chain also complicates keeping control of goods and tracking distribution beyond a certain point.

OFAC Warns of Deceptive Practices in Russian Oil Trade

➤ Treasury's Office of Foreign Assets Control (OFAC) has issued a warning to shipowners, protection and indemnity clubs, and flagging registries about deceptive practices involving Russian oil exports.

OFAC is aware of reports that crudes exported via Pacific ports in the Russian Federation, such as Kozmino, may be trading above the price cap and using covered services provided by U.S. persons. These service providers may be unknowingly involved in the trade due to false or incomplete documentation and other deceptive practices.

One such deceptive practice is the manipulation of Automatic Identification Systems (AIS) on tankers, a practice known as "spoofing." This tactic is used to disguise port calls to Kozmino or other Russian Federation eastern coastline ports. Spoofing can also be employed to mask ship-to-ship transfers.

U.S. service providers are urged to view AIS manipulation as evidence of potential evasion of the price cap.

For commodities brokers and oil traders, OFAC emphasizes the importance of transparent shipping costs. Shipping, freight, customs, and insurance costs should be invoiced separately from the purchase price of Russian oil and must be at commercially reasonable rates.

Failure to itemize these costs can be used to obscure the fact that Russian oil was purchased above the price cap. Refusal by a counterparty to provide documentation showing that the oil was purchased at or below the price cap should be considered a red flag for potential evasion.

Russian Success in Circumventing Western Sanctions

➤ A paper issued by CSIS, a Washington think tank, details progress to date of the Putin regime in maintaining advanced technology supply lines in the face of Allied sanctions.

The report assesses the impact of Western sanctions and allied export regulations on Russia's defense sector, focusing on the production of core weapons and systems. It also examines the Kremlin's efforts to mitigate the effects of the sanctions regime through import substitution and sanctions-evasion techniques.

The Kremlin's import substitution efforts have been largely unsuccessful due to the ambitious nature of these projects and the limited domestic capabilities of Russia's defense industry. As a result, Russia has been forced to rely on illicit supply chains and sanctions-evading land corridors to obtain restricted foreign components and technologies.

Iran and China have been key suppliers for Russia, with Iran sharing its experience in circumventing Western sanctions. Land corridors involving **post-Soviet countries, the Balkan Peninsula, and Turkey** have also been utilized. While these alternative routes have been somewhat successful in maintaining the flow of restricted components, they also come with increased costs, volatility, and time consumption for Moscow.

The report concludes that Russia is likely to opt for a slower-paced attritional campaign in Ukraine.

Recommendations to close loopholes and strengthen the effectiveness of sanctions include:

- Continuously supply Ukraine with higher-end military equipment at a pace that exceeds Russia's production rate.
- Identify and target illicit networks and individuals involved in sanctions-evasion efforts, and use U.S. leverage in the post-Soviet region.
- Restrict existing transactions with Russian and Russia-linked defense companies and their affiliates.
- Eliminate loopholes that allow some Western companies to import equipment into Russia by extending past contracts that preceded the imposition of sanctions.
- Work towards creating an EU-level OFAC equivalent to monitor sanctions implementation and compliance,.

Oil tanker in the port of Murmansk, Russia.

PETER PROKOSCH

OFAC BRIEFS

Sanctions Reaction to Hostage Taking in Russia and Iran

➤ Treasury's Office of Foreign Assets Control (OFAC) has imposed sanctions on four senior officials of Iran's Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO) in a groundbreaking move.

This marks the first time Executive Order (E.O.) 14078 has been employed to penalize individuals involved in the hostage-taking or wrongful detention of U.S. nationals in Iran. The IRGC-IO has been designated by the State Department for its role in suppressing protests, arresting dissidents, and detaining and interrogating prisoners in Evin Prison.

In addition to the action against Iran, OFAC has implemented the State Department's designation of Russia's Federal Security Service (FSB) for its involvement in the wrongful detention of U.S. nationals abroad.

E.O. 14078 draws its authority from the 2020 Robert Levinson Hostage Recovery and Hostage Taking Accountability Act, recognizing the Levinson family's and others' efforts in turning their hardships into meaningful action.

PYONGYANG MORANBONG EDITORIAL BUREAU

More Russian Sanctions; Entities Named

➤ Treasury, Commerce, State and the UK's Foreign Office launched a coordinated expansion of sanctions on the Russian military-industrial complex, as well as the personal holdings and advisors of a prominent oligarch.

Additionally, the State Department is sanctioning two Russian entities that support the militarization and indoctrination of schoolchildren.

Treasury's Office of Foreign Assets Control (OFAC) and UK officials are targeting the facilitation network of **Alisher Usmanov**, one of Russia's wealthiest billionaires, who is subject to sanctions in multiple jurisdictions.

The UK actions against the same individuals drew attention to the prominent role of **Roman Amramovich,** whose billions in trust were cleverly reorganized shortly before sanctions were imposed.

OFAC is designating 25 individuals and 29 entities with touchpoints in 20 jurisdictions.

The U.S. Department of State is concurrently designating several entities operating in the defense sector of the Russian Federation economy, entities supporting Russia's war against Ukraine, and additional entities associated with Russia's State Atomic Energy Corporation.

OFAC Names North Korean Bankers

➤ Treasury's Office of Foreign Assets Control (OFAC) has sanctioned three individuals for providing support to North Korea through illicit financing and malicious cyber activity.

The Democratic People's Republic of Korea (DPRK) is accused of laundering stolen virtual currency and deploying information technology (IT) workers to fraudulently obtain employment to generate revenue for the regime's unlawful weapons of mass destruction and ballistic missile programs. These workers use fake personas to apply for jobs and request payment in virtual currency, which is then sent through a complicated laundering pattern back to the DPRK.

The U.S. has taken these actions in close coordination with South Korea.

"The DPRK's use of illicit facilitation networks to access the international financial system and generate revenue using virtual currency for the regime's unlawful weapons of mass destruction and ballistic missile programs directly threatens international security," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.

He added that the US and its partners are committed to safeguarding the international financial system, particularly in light of the three intercontinental ballistic missile (ICBM) launches this year.

Wu Huihui and **Cheng Hung Man** have been designated for providing material support to the Lazarus Group, which is controlled by the DPRK's primary intelligence bureau, the Reconnaissance General Bureau. The Lazarus Group has been involved in cyber espionage, data theft, monetary heists, and destructive malware operations. It is also responsible for the largest virtual currency heist to date, stealing almost $620 million from a blockchain project linked to the online game Axie Infinity.

Sim Hyon Sop has been designated for acting on behalf of the Korea Kwangson Banking Corp (KKBC), an entity that provides financial services in support of both Tanchon Commercial Bank and Korea Hyoksin Trading Corporation.

ROBERT SCOBLE

Microsoft Settles with OFAC and BIS for Violations

Screening Failures Cited

Microsoft has agreed to pay $3.3 million to settle potential civil liability relating to exporting services or software to comprehensively sanctioned jurisdictions and Specially Designated Nationals (SDNs) in violation of OFAC's Cuba, Iran, Syria, and Ukraine-/Russia-Related sanctions programs.

The majority of the apparent violations involved blocked Russian entities or individuals in the Crimea region of Ukraine, resulting from **Microsoft Entities' failure to identify and prevent their products' usage by prohibited parties.**

Between July 2012 and April 2019, Microsoft Entities were involved in 1,339 apparent violations of multiple OFAC sanctions programs. They sold and activated software licenses and provided related services worth $12,105,189.79 to Specially Designated Nationals (SDNs), blocked persons, and end users in Cuba, Iran, Syria, Russia, and the Crimea region of Ukraine. The apparent violations were committed through servers and systems located in the United States and Ireland.

The violations occurred when Microsoft Entities engaged with third-party distributors and resellers to sell Microsoft software products. In Russia, Microsoft Entities employed an indirect resale model through third-party Licensing Solution Partners (LSPs). Microsoft Russia collaborated with LSPs to develop sales leads and ne-

Continues on next page

Continued from previous page

gotiate bulk sales agreements with end customers. Microsoft Ireland billed the LSPs annually for licenses supplied, and the LSPs separately billed and collected payment from end customers.

End customers downloaded or accessed the software, installed it on devices or networks, and activated it using a product key. The processes for software downloads, license activations, product key verifications, and subsequent usages relied on U.S.-based servers and systems managed by personnel in the U.S. or third countries. End customers blocked under the Ukraine sanctions program also benefited from services processed through Microsoft's U.S.-based servers and systems.

When Microsoft Entities supported sales or arranged services for prohibited parties through third-party distributors and resellers, they provided prohibited software and services to SDNs, blocked persons, and end customers in sanctioned jurisdictions. The software and related services were ineligible for any general licenses or other exemptions.

The causes of these apparent violations included the lack of complete or accurate information on the identities of end customers for Microsoft's products. In some instances, Microsoft Russia employees even intentionally circumvented Microsoft's screening controls to hide the identity of the ultimate end customers.

Holistic risk assessments, especially for companies operating in high-risk jurisdictions, are vital to avoid engaging in business dealings with prohibited parties.

During the time period of the apparent violations, there were shortcomings in Microsoft's restricted-party screening. For example, Microsoft's screening architecture did not aggregate information known to Microsoft, such as an address, name, and tax-identification number, across its databases to identify SDNs or blocked persons. Microsoft also failed to timely screen and evaluate pre-existing customers following changes to OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) and implement timely corrective measures.

Microsoft's screening against restricted-party lists did not identify blocked parties not specifically listed on the SDN List, but owned 50 percent or more by SDNs, or SDNs' Cyrillic or Chinese names. Many customers in Russia and China provided order and customer information in their native scripts. These failures also included missing common variations of the restricted party names.

In total, the Microsoft Entities appear to have engaged in 54 apparent violations of the Cuban Assets Control Regulations, 30 apparent violations of the Iranian Transactions and Sanctions Regulations, 3 apparent violations of the Syrian Sanctions Regulations, and 1,252 apparent violations of the Ukraine-/Russia Related Sanctions Regulations.

The settlement amount reflects OFAC's determination that the conduct was non-egregious, voluntarily self-disclosed, and significant remedial measures were taken by Microsoft upon discovering the apparent violations. This action was part of a joint administrative enforcement effort with the Bureau of Industry and Security (BIS), which settled with Microsoft for $624,013 for related violations of the Export Administration Regulations

The statutory maximum civil monetary penalty for Microsoft's apparent violations of OFAC sanctions is $404,646,121.89. Microsoft voluntarily self-disclosed the apparent violations, which were deemed non-egregious, resulting in a base civil monetary penalty of $5,960,531.72. The settlement amount of $2,980,265.86 takes into account the General Factors under the Enforcement Guidelines. Aggravating factors include the reckless disregard for U.S. sanctions, harm to U.S. foreign policy objectives, and Microsoft's position as a leading technology company.

Mitigating factors include the absence of knowledge by U.S. offices or management, Microsoft's voluntary self-disclosure and cooperation, termination of SDNs or blocked persons' accounts, and significant remedial measures and enhancements to its sanctions compliance program.

Companies with sophisticated technology operations and a global customer base should ensure their sanctions compliance controls remain commensurate with the risks and leverage appropriate technological compliance solutions.

Holistic risk assessments, especially for companies operating in high-risk jurisdictions, are vital to avoid engaging in business dealings with prohibited parties.

Seagate Fined $300 Million for Huawei Violations

Largest Standalone Administrative Penalty in BIS History

COMMERCE'S BUREAU OF INDUSTRY AND SECURITY (BIS) has imposed a $300 million civil penalty on Seagate Technology LLC and its Singapore subsidiary for alleged violations of U.S. export controls related to selling hard disk drives (HDDs) to Huawei Technologies Co. Ltd.

This penalty is the largest standalone administrative penalty in BIS history and includes a multi-year audit requirement and a five-year suspended Denial Order.

In August 2020, BIS imposed controls over certain foreign-produced items related to Huawei. Despite this, in September 2020, Seagate announced it would continue to do business with Huawei.

Seagate became Huawei's sole source provider of HDDs after its two competitors ceased sales to the Chinese company. Seagate subsequently entered into a three-year Strategic Cooperation Agreement with Huawei, granting the company priority over other Huawei suppliers.

BIS's investigation found that Seagate allegedly violated the Export Administration Regulations (EAR) by ordering or causing the reexport, export from abroad, or transfer (in-country) of over 7.4 million HDDs subject to the Huawei foreign direct product (FDP) rule without BIS authorization.

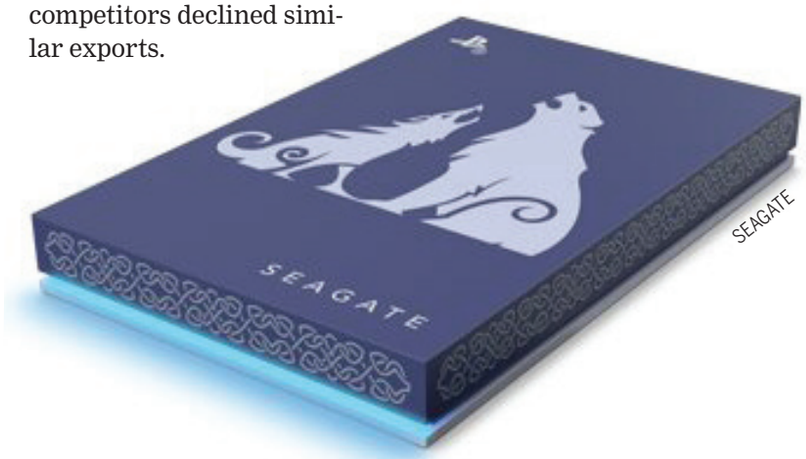
"Even after Huawei was placed on the Entity List for conduct inimical to our national security, and its competitors had stopped selling to them due to our foreign direct product rule, Seagate continued sending hard disk drives to Huawei," said **Assistant Secretary for Export Enforcement Matthew S. Axelrod.** "Today's action is the consequence: the largest standalone administrative resolution in our agency's history. This settlement is a clarion call about the need for companies to comply rigorously with BIS export rules, as our enforcement team works to ensure both our national security and a level playing field."

"Those who would violate our FDP rule restrictions are now on notice that these cases will be investigated and charged, as appropriate," said **Director of the Office of Export Enforcement John Sonderman.** "Any company exporting to an entity subject to the additional FDP rule restrictions needs to evaluate its entire manufacturing process to determine if specified U.S. technologies or software were used in building the essential tools used in production. Companies that discover violations should submit voluntary self-disclosures to OEE."

BIS issued an order against Seagate imposing a $300 million administrative penalty, a mandatory multi-year audit requirement, and a five-year suspended Denial Order. Seagate admitted to the conduct set forth in the Proposed Charging Letter involving both the U.S. and Singapore entities.

Between August 17, 2020, and September 29, 2021, Seagate allegedly engaged in prohibited conduct on 429 occasions, exporting approximately 7,420,496 foreign-produced HDDs, valued at about $1.1 billion, to Huawei entities listed on the BIS Entity List or where such entities were a party to a transaction without BIS authorization. The other two HDD manufacturers had publicly ceased sales to Huawei, but Seagate continued transactions involving the Chinese company. BIS's $300 million penalty is over twice the estimated net profits from the alleged illegal exports to Huawei.

As transactions progressed, Seagate repeatedly authorized extending lines of credit to Huawei totaling more than $1 billion between January and September 2021, resulting in an increasing volume of HDD exports. In March 2021, Seagate and Huawei entered into a Long-Term Agreement involving a purchase agreement of over 5 million HDDs, naming Seagate a "key strategic supplier." Meanwhile, Seagate's competitors declined similar exports.



BAT Toasted for Pyongyang Cigarette Scheme

➤ London-based tobacco giant, British American Tobacco p.l.c. (BAT), has agreed to pay more than $600 million to settle civil charges related to alleged violations of the North Korea and Weapons of Mass Destruction Proliferators Sanctions Regulations, according to a statements from the US Treasury's Office of Foreign Assets Control (OFAC) and the Justice Department.

The settlement is related to BAT's role in exporting tobacco and related products to North Korea and receiving payment for those exports through the US financial system, and its subsidiary's use of US financial institutions to receive or otherwise process US dollar-denominated payments for its sale of cigarettes to the DPRK Embassy in Singapore. This caused US financial institutions to process wire transfers that contained the blocked property interests of sanctioned North Korean banks and to export financial services and facilitate the exportation of tobacco to North Korea.

OFAC determined that these apparent violations were egregious and not voluntarily self-disclosed, resulting in the statutory maximum civil monetary penalty.

The apparent conspiracy formed by BAT and its subsidiaries, the North Korea Company, and the Singapore Company caused U.S. financial institutions to process 228 payments between the North Korea Company and the Singapore Company totaling approximately $251,631,903—transactions in which two blocked entities, Korea Kwangson Banking Corporation (KKBC) and Foreign Trade Bank (FTB), had an interest.

BATM's sale of cigarettes to the DPRK Embassy in Singapore further caused U.S. financial institutions to receive or otherwise process an additional 15 payments totaling $29,685.72. This conduct resulted in one apparent violation of the Weapons of Mass Destruction Proliferators Sanctions Regulations and 15 apparent violations of the North Korea Sanctions Regulations.

According to the OFAC statement, BAT's apparent violations began in 2001, when its Singapore subsidiary, British-American Tobacco Marketing (Singapore) PTE Ltd., and a North Korean company established a joint venture company in North Korea to manufacture and distribute BAT cigarettes.

"In 2007, British American Tobacco announced that it had ended all tobacco sales in North Korea as required by U.S. sanctions. In fact, the company continued to break the law by doing business in the DPRK using a third-party company under the control of its subsidiary. Between 2007 and 2017, this third-party company sold tobacco products to North Korea and received approximately $428 million dollars. This money was then funneled back to British American Tobacco" said Assistant Attorney General for National Security Matt Olsen announcing the settlement.

BRITISH AMERICAN TOBACCO, PLC

The settlement amount for the statutory maximum reflects OFAC's consideration of the General Factors under the Enforcement Guidelines. OFAC determined **several aggravating factors,** including

- that BAT and its subsidiaries willfully conspired to transfer hundreds of millions of dollars through U.S. banks in which sanctioned North Korean banks had an interest,
- that they concealed their North Korea-related business,
- that BAT management had actual knowledge regarding the apparent conspiracy,
- that BAT's apparent violations helped North Korea establish and operate a cigarette manufacturing business, and
- that BAT is a large and sophisticated international company operating in approximately 180 markets around the world.

In addition to the OFAC settlement, BAT is also required to pay a penalty of $503,263,807 for its apparent conspiracy violation of the Weapons of Mass Destruction Proliferators Sanctions Regulations, as assessed by the US Department of Justice (DOJ). BAT's obligation to pay this penalty shall be deemed satisfied by payment of a greater amount in satisfaction of penalties assessed by DOJ arising out of the same pattern of conduct during the same time period.

BRIEFS

Oil Services Firm Settles Over Angolan Bribery

➤ The U.S. Securities and Exchange Commission (SEC) has settled violations of the Foreign Corrupt Practices Act (FCPA) with **Frank's International**, a global oil services company. Between January 2008 and October 2014, Frank's paid commissions to a sales agent in Angola, knowing there was a high probability the agent would use the funds to bribe Angolan government officials to influence the award of oil and natural gas services contracts.

Frank's sought to provide tubular services and technology to support the drilling of wells in Angola's offshore blocks. Angolan state-owned oil company, Sonangol blocked Frank's hiring, and the company was informed that it could regain favor by establishing a consulting company and paying 5% of the contract value to the consulting company for the benefit of high-ranking Sonangol officials.

Instead, Frank's retained an Angolan agent with close ties to the Angolan government. The company continued to make payments to the agent without conducting due diligence or having a contract in place. The agent funneled a portion of the money received from Frank's to the Angolan government official, securing new contracts for Frank's in the process.

Frank's recorded these illicit payments as "business expenses," "entertainment and meals," and "commissions" in its books and records. The company continued to use the agent and provide benefits to the Angolan official even after becoming a public company. Between 2008 and 2014, the agent's businesses received approximately $5.5 million from Frank's, a portion of which was paid to the Angolan official.

In settling the FCPA violations, the SEC has required Frank's to address its internal controls and conduct a thorough internal investigation to identify all individuals involved in the corrupt practices. The Settlement includes disgorgement of $4,176,858 and prejudgment interest of $821,863 and a civil money penalty of $3,000,000.

General Motors Settles Over Immigration-Related Discrimination

➤ The U.S. Justice Department has reached a settlement with **General Motors** (GM) over alleged discrimination against non-U.S. citizens in violation of the Immigration and Nationality Act (INA).

The department's investigation determined that GM's export compliance assessments improperly required lawful permanent residents to provide an unexpired foreign passport as a condition of employment, creating a discriminatory barrier in the hiring process.

The company also improperly combined its process for verifying workers' permission to work in the U.S. with its export compliance assessment.

In response to the investigation, the Justice Department is releasing a new fact sheet to help employers avoid citizenship status discrimination when complying with export control laws, such as the International Traffic in Arms Regulations and the Export Administration Regulations.

Under the terms of the settlement, GM will pay $365,000 in civil penalties, train its personnel on the INA's requirements, revise its employment policies, and be subject to departmental monitoring and reporting requirements.

GM must also separate its process for verifying permission to work in the U.S. from its export compliance assessment process and stop requiring lawful permanent residents to present foreign passports as a condition of employment.

$826K Forfeited in Failed Russian Machine Tool Sale

➤ A federal court has ordered the forfeiture of approximately $826,000 connected to an attempt to smuggle a dual-use export-controlled item to Russia. The high-precision jig grinder, manufactured in Connecticut, was intercepted in Riga, Latvia. The machine is subject to export restrictions due to its potential applications in nuclear proliferation and defense programs.

The alleged smuggling operation began in 2018 and involved a Latvia-based corporation working with **By Trade OU**, an Estonia-based company, as well as individuals in Russia and a Russia-based company. These parties conspired to violate U.S. export laws and regulations, including the Export Control Reform Act of 2018 and the Export Administration Regulations (EAR).

By Trade OU pleaded guilty to one count of conspiracy to violate the Export Control Reform Act and one count of international money laundering conspiracy. The company admitted to receiving funds from a Russian company to purchase the jig grinder on its behalf from the Latvian company that had arranged to buy the device from the manufacturer.

U.S. District Judge Victor A. Bolden ordered the forfeiture of $484,696, which had been delivered to the manufacturer as part of the attempted purchase, as well as €312,192.44 (approximately $342,000) seized from By Trade OU.