April 2024 | Vol. 38, No. 4

EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:

Export Controls Face East

Inside: Standing room only at BIS Update Conference

WELCOME TO YOUR NEW

EXPORT PRACTITIONER™

IN PRINT | VIA EMAIL | ONLINE

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 703-283-5220.

Scan or Click For Our Top Stories:

VISIT ONLINE AT EXPORTPRAC.COM

EP
THE EXPORT PRACTITIONER™
April 2024 | VOL. 38, NO. 4

EXPORT PRACTITIONER

FEATURE

POLICY

ENFORCEMENT

SANCTIONS

ON THE COVER: Lincoln Memorial Reflecting Pool, facing east towards the Washington Monument. ADOBESTOCK / STEHEAP

The Export Practitioner
www.exportprac.com

Mailing Address: P.O. Box 7592, Arlington, VA 22207
Telephone: 703.283.5220
E-Mail: info@traderegs.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

BIS UPDATE CONFERENCE

Standing Room Only: 'We are cranking folks'

The Commerce Department's Bureau of Industry and Security 2024 Update Conference kicked off to a full house in Washington, with over 1,100 attendees registered and many breakout sessions extended to overflow rooms with video feeds.

While Commerce Secretary Gina Raimondo was unable to attend in person, **Under Secretary of Commerce for Industry and Security Alan Estevez** greeted attendees with a recap of the work undertaken since the last conference in 2022, and insights on where things are headed.

"We are cranking folks," Mr. Estevez told the audience. "As is often the case, things happen gradually — then seemingly all at once. That is the story of the past few years."

"We are asking the private sector to step up more than it has, and even if you have not heard from us directly, we need you to be part of the solution.

"Traditional due diligence is not sufficient—especially if your company or your clients have complicated distribution networks. Government and industry both need to show a commitment at the highest levels and continue to devote resources to detecting red flags, vetting intermediaries, tracking controlled product, and sharing information and best practices.

"I want to be clear: Export controls are a national security tool, not an economic protectionist tool. BIS has been called upon to apply export controls on items that the PRC is seeking to obtain in order to advance its military modernization and its human rights abuses.

"Military advantage is now being sought through advanced computing power — supercomputers that can manage and manipulate vast amounts of data, artificial intelligence (AI) that speeds military decision-making, and a host of other activities that rely on certain advanced chips and the ability to make or obtain them.

"The Department of Commerce employs an 'offense/defense' approach — BIS's work is the defense. The offense is the Department's work, led by other bureaus, to implement the CHIPS and Science Act and a host of other laws, which will ensure that U.S. technological leadership continues to advance and that the benefits of this advancement are widely distributed across our nation.

EXPORT PRACTITIONER

Assistant Secretary for Export Enforcement Matthew Axelrod, right, and Under Secretary of Commerce for Industry and Security Alan Estevez at the BIS Update Conference in March.

New Enforcement Initiatives

Assistant Secretary for Export Enforcement Matthew Axelrod announced four new Enforcement Initiatives at the 2024 Update Conference on Export Controls and Policy.

In his plenary address, Mr. Axelrod introduced new guidance for the Freight Forwarder community, an updated compendium of enforcement examples, an antiboycott blacklist, and enhanced outreach to manufacturers and distributors of restricted good discovered on the battlefield in Ukraine.

Freight Forwarder Guidance

Axelrod announced updated guidance for freight forwarders, developed after discussions with industry stakeholders. This document outlines roles, responsibilities, and best practices to help ensure compliance with export and antiboycott regulations. [11973]

Case Examples Digest

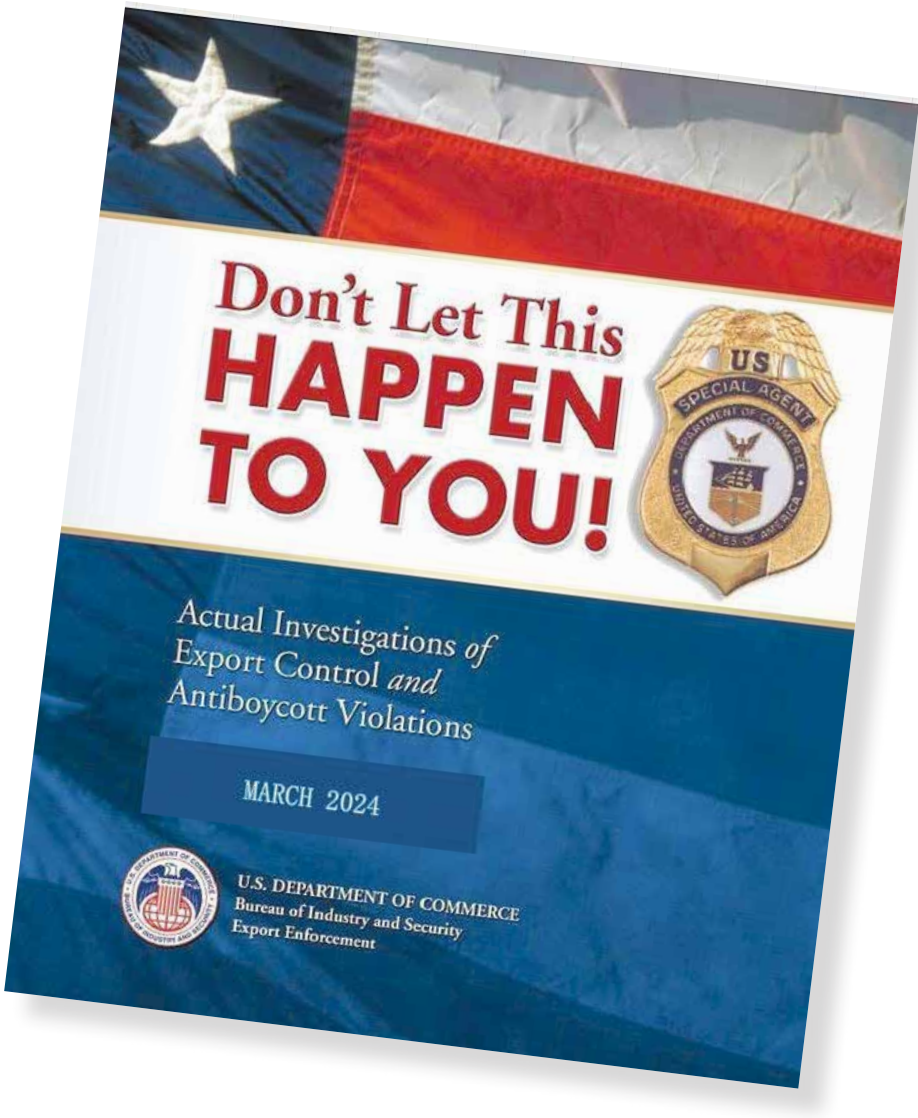
An updated "Don't Let This Happen to You" compendium has been published, highlighting recent enforcement actions to illustrate the risks of non-compliance. [11974]

Antiboycott Blacklist

A new blacklist identifies parties requesting boycott actions, compiled from revised reporting forms. This list is intended as a compliance resource for businesses to avoid involvement in unsanctioned boycotts. "We encourage you to diligently review transaction documents from all sources," said Axelrod, "but especially transaction documents with these parties, given that they've been identified by others as a source of boycott requests. [11967]

Red Flag Outreach

To counter the flow of Western components into Russia, where they're being used in military equipment, a focused initiative was launched to pinpoint and alert U.S. companies about their customers who persist in shipping critical items to Russia. This effort involved issuing "red flag" letters based on customs data, urging these companies to apply extra scrutiny and enhance their export controls.



"Don't Let This Happen to You," an updated version of a compendium of case examples highlighting criminal and administrative enforcement efforts.

Extending this initiative, information from datasets on Russian imports has been shared with U.S. manufacturers and distributors **who make and sell products that continue to be found in recovered missiles and drones inside Ukraine**, identifying over 600 foreign entities continuing such shipments. These companies have been advised to cease dealings with the listed entities to prevent their products from being rerouted to Russia..

"That's in addition to the work our Under Sec-

Continues on next page

'Our goal is to encourage and incentivize investment in compliance on the front end, while also emphasizing the financial and reputational cost of facing an enforcement action on the back end.'

Matthew Axelrod, Assistant Secretary for Export Enforcement

Continued from previous page

retary has been doing with his counterparts from the Departments of State and the Treasury — **reaching out directly to senior leaders at U.S. companies** to discuss further steps they can take to help prevent their products from ending up inside Russian weapons," said Mr. Axelrod.

Collaboration & Consequences

Mr. Axelrod emphasized the collaboration his team has developed with other enforcement activities, as well as with industry. "Effective compliance is the first component of effective enforcement. It's the time, money, and effort that you put into your compliance programs that stop sensitive U.S. technology from going to our adversaries.

"Our goal is to encourage and incentivize investment in compliance on the front end, while also emphasizing the financial and reputational cost of facing an enforcement action on the back end."

Compliance on the front end

Starting with front end compliance, we've conducted extensive outreach to educate industry and academia about our policies and procedures, as well as the trends we're seeing. With regard to Russia, for example, we've published best practice guidance, including a sample end-use certification form, for exporters to use to help prevent diversion of high-priority "battlefield items," like microelectronics and ball bearings, to the Russian war machine. We've also conducted over 800 outreaches to the exporting community about the new restrictions.

More broadly, we've issued more than a dozen advisory notes, guidance documents, and alerts in coordination with other government agencies like the Departments of Justice, the Treasury, Homeland Security, and State.

Just a few weeks ago, for example, we published a tri-seal advisory with the Departments of Justice and the Treasury on the **applicability of our respective controls and laws to non-U.S. entities.** The advisory makes clear that parties outside the United States are not exempt from U.S. export controls or BIS enforcement when it comes to reexporting items subject to our regulations. '

For the academic community, we've gone a step beyond guidance documents. Over the last year, we expanded our Academic Outreach Initiative from 20 to 29 universities. The Initiative is designed to help academic institutions maintain an open, collaborative research environment in a way that also helps protect them from national security risk.

Voluntary Self Disclosure

In addition, we've updated our enforcement policies to help drive compliance, including our policies on voluntary self-disclosures (VSDs). Last April, we clarified our VSD policies with the goal of driving additional disclosures of significant possible violations of the Export Administration Regulations (EAR).

When a company thinks about whether or not to disclose an apparent violation, we want them to consider two additional factors: **first**, that a deliberate non-disclosure of a significant possible violation of the EAR is now considered an aggravating factor under our penalty guidelines; and **second**, that if you don't tell us yourself, your competitor might — because we now award them future cooperation credit for doing so.

These policies are working. Since their implementation, we've seen increases both in the number of VSDs involving potentially serious violations and in disclosures about the misconduct of others.

More recently, in January, we reduced the administrative burden associated with submitting VSDs for more minor or technical violations. By simplifying the disclosure process for minor or

technical violations, we're encouraging companies to focus their resources on the more serious violations, where we continue to recommend a thorough review for the preceding five years.

Enforcement on the back end

Mitigating national security risk costs money, one way or the other. We'd much prefer that you spend that money investing in compliance on the front end rather than paying it in fines on the back end. But either way, it's going to cost something.

Lest you be tempted to dismiss this as just "tough talk," last year saw our highest number ever of convictions, temporary denial orders (TDOs), and post-conviction denial orders. And you can expect our rapid enforcement tempo to continue.

The BIS 2024 Update Conference kicked off to a full house in Washington.
EXPORT PRACTITIONER

FinCEN

Our work has benefitted from leads generated out of Suspicious Activity Reports (SARs) filed with FinCEN. Whereas financial institutions previously had no systematic way to indicate suspected export control violations when filing SARs, FinCEN has now created two "key terms" for institutions to use — one for Russia diversion and one for export control evasion globally.

To date, we have reviewed over 700 filed SARs, and we have been able to action more than 100 of those filings in various ways, including by sending leads to our enforcement agents, advancing existing cases, and developing Entity List packages.

Antiboycott Initiatives: New Blacklist

Since last Update, we've also enhanced our antiboycott enforcement efforts to ensure that U.S. companies are not used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel. In October 2022, we raised our penalties and instituted a requirement that companies entering into settlement agreements for antiboycott violations admit to a statement of facts outlining their conduct. Last July, we announced a renewed focus on foreign subsidiaries of U.S. companies and noted that we would explore additional ways to deter foreign parties from issuing or making boycott requests. We also modified the boycott reporting form to require submitters to indicate the identity of the requesting party.

The Commerce Department has introduced a public list of entities identified as having made a boycott-related request in reports received by BIS. The list is posted on the Office of Antiboycott Compliance (OAC) webpage with the objective of helping U.S. persons comply with the antiboycott regulations set forth in Part 760 of the Export Administration Regulations, 15 CFR Parts 730-774 (EAR).

Each entity on this list has been recently reported to BIS on a boycott request report form, as required by Section 760.5 of the EAR, as having made a boycott-related request in connection with a transaction in the interstate or foreign commerce of the United States. The list is not exhaustive and will be updated quarterly.

Again, I'd much rather you comply with the export rules on the front. Better for you, since you don't want your product found on the battlefield and Ukraine or your technology used by an authoritarian government to repress its population. And it's better for us because we don't want your technology or product being used that way either. [11977]

BIS Export Administration: New Organization

Export Administration is getting a new leadership framework, including the creation of Deputy Assistant Secretary roles for Strategic Trade and Technology Security, under the oversight of the newly elevated Principal Deputy Assistant Secretary Matt Borman.

The Changes involve dividing EA's functions into two primary channels: Strategic Trade, focusing on licensing, outreach, and training, and Technology Security, which encompasses defense industrial base (DIB) responsibilities, analysis, and regulatory work.

EXPORT PRACTITIONER

Thea Kendler talks with reporters at the BIS Update Conference.

Assistant Secretary for Export Administration Thea Rozman Kendler announced the organizational moves in a plenary address to the BIS Update Conference last week.

[remarks edited for brevity]

"Our increasing focus on preventing adversaries from harnessing the potential of emerging technologies like artificial intelligence has not distracted from our traditional nonproliferation focus. Even as we expanded advanced computing controls on the PRC, we also expanded nuclear nonproliferation controls to ensure that deuterium, graphite, and other nuclear-related items are only being used in the PRC for peaceful activities such as commercial nuclear power generation, medical developments, and non-military industries.

"EA had a very busy 2023. We processed nearly 40,000 license applications with an average processing time of 32 days, not including applications for the PRC. The Operating Committee heard 614 applications, the Advisory Committee for Export Policy reviewed 45, and no cases were elevated to the Export Advisory Review Board. We published 45 rules, with thousands of pages, as you know, and added 466 entities to the Entity List.

Organizational Repositioning

Internal review recognized two main channels of activity in EA: **First, Strategic Trade** — this is our licensing functions, outreach, and training mission. **Second, Technology Security** — this is our DIB responsibilities, as well as all of the analysis we do — whether on licensing and trade data, industry research, or intelligence — and our 232 work.

We formally created two Deputy Assistant Secretary (DAS) roles to lead this work — a DAS for Strategic Trade, and a DAS for Technology Security. Above them, is the Principal Deputy Assistant Secretary, a position to which we've elevated national treasure **Matt Borman.**

In office organizational terms, the **DAS for Strategic Trade** will oversee the Office of National Security and Technology Transfer Controls, Office of Nonproliferation and Treaty Compliance, and the Office of Exporter Services.

The new **DAS for Technology Security** will be responsible for Office of Strategic Industries and Economic Security and the Office of Technology Evaluation. Those are the topline changes.

Export Control Reform Act Section 1758 charges us with identifying and implementing appropriate controls on emerging and foundational technologies essential to national security. This work, as well as foreign technology analysis and other research efforts designed to help assess the effectiveness of our export controls, will be formalized under the DAS for Technology Security.

Formalizing a Technology Security branch of EA is essential for moving BIS from its historic focus on export control regulations towards a holistic approach of assessing the intersection of tech ecosystems, export control authorities, and national security and foreign policy goals.

Under our new PDAS, we formed an International Policy Office (IPO). IPO leads EA's increasing focus on engaging on a plurilateral and bilateral basis to address evolving threats, helps institutionalize

the many plurilateral and bilateral relationships we've developed over the last two years, and enables country-specific analysis not necessarily tied to a specific technology or multilateral regime.

Strategic Trade Authorization & Validated End User

"You saw some of our efforts in rules published last year removing license requirements for certain items and making it easier to use license exceptions for exports to close partners. **Related to that, you can expect a final Strategic Trade Authorization rule this summer.**

We're looking for ways to make it easier for industry to work with international partners that embrace the principles of export controls. Many of your companies already maintain operations in countries that don't have export control laws and regulations in place.

For those of you with multinational operations, consider the example of a Validated End User, or "VEU," operating in India. As a VEU, this company is eligible to receive advanced tech exports without waiting for suppliers to obtain a license from BIS.

The VEU process allows for more certainty and reliability regarding the receipt of items subject to the EAR that are include in their VEU authorization. It does not have an expiration date like a license, and can be made available to re-exporters. We are working through different scenarios to see how authorization VEU could be further utilized around the world. We welcome your feedback on this.

Wassenaar Alternatives

The best way to truly keep potentially dangerous technologies and know-how out of the hands of bad actors is to work together.

This is the approach we have adopted in building the Global Export Control Coalition, focused on using all aspects of export controls to degrade Russia's military capabilities, as well as those of enablers such as Belarus and Iran. This coalition — led by the EC, Japan, UK and the U.S. — enabled us to drive new approaches to lower-level commodity controls on Russia and its partners, using Harmonized Systems (HS) codes to parse EAR99 items.

SUMMIT ART CREATIONS

It's also the approach we've applied to Russia's efforts to stymie Wassenaar Arrangement (WA) progress. For two years now, Russia has stood in the way of new multilateral controls being adopted through the WA. And so — through the efforts of our State Department colleagues and leading international partners — we have been creative with our workarounds. **You'll see us publish new plurilateral controls stemming from 2022 and 2023 WA discussions in the near term.**

Emphasis on Data

The new structure of EA and our foreign government and industry engagements, reflect the data-driven nature of our mission. We at Commerce don't rely on State, Defense, or Energy to find derogatory information for us. Our licensing officers assess applications based on their familiarity with technology, industry, and regional issues, as well as intel. To this end, we in EA are putting resources into improving our access to intel and collaboration with the intelligence community.

Take our advance chip and SME rules — our licensing officers, many of whom are highly-trained engineers — worked with the intelligence community to understand the threat posed by the PRC's access to advanced integrated circuits.

We also rely on the intelligence community to help us make the case to our allies that the technology we care about will contribute to programs that harm our national security. The more we can share intelligence about technology risks with our close partners, the more we can bring them on board with our technology control proposals. [11978]

The new DAS for Technology Security will be responsible for Office of Strategic Industries and Economic Security and the Office of Technology Evaluation.

Lombard Street, San Francisco, California. The ABAs 39th National Institute on White Collar Crime was held in San Francisco this year.

ADOBESTOCK

Monaco Announces Whistleblower Program

Deputy Attorney General **Lisa Monaco** told the American Bar Association's 39th National Institute on White Collar Crime to expect a new focus on whistleblowing, and that "AI resilience" is an element evaluating a firm's compliance readiness.

"Going back to the days of "Wanted" posters across the Old West, law enforcement has long offered rewards to coax tipsters out of the woodwork. And today, we're announcing a program to update how DOJ uses monetary rewards to strengthen our corporate enforcement efforts.

So we're planning something new: a DOJ-run whistleblower rewards program. Today, we're launching a 90-day sprint to develop and implement a pilot program, with a formal start date later this year.

It's important to underscore a central aspect of all whistleblower programs. To be eligible for a reward, you have to tell us something we didn't already know. You have to be the first in the door. When everyone needs to be first in the door, no one wants to be second — regardless of whether they're an innocent whistleblower, a potential defendant looking to minimize criminal exposure, or the audit committee of a company where the misconduct took place.

Compliance officers should take note. When our prosecutors assess a company's compliance program — as they do in all corporate resolutions — they consider how well the program mitigates the company's most significant risks. And for a growing number of businesses, that now includes the risk of misusing AI.

That's why, going forward and wherever applicable, our prosecutors will assess a company's ability to manage AI-related risks as part of its overall compliance efforts. To that end, I have directed the Criminal Division to incorporate assessment of disruptive technology risks — including risks associated with AI — into its guidance on Evaluation of Corporate Compliance Programs.

Executives Targeted

Acting Assistant Attorney General **Nicole M. Argentieri** noted the increased emphasis on personal

responsibility in her speech at the ABA Conference:

"Our prosecutors are trying more white collar cases against individuals than ever before.... In 2023, about a quarter of the more than 250 individuals charged by Criminal Division prosecutors in white collar cases were corporate executives, lawyers, or medical professionals.

"In 2023, we received nearly twice as many disclosures as in 2021. We expect this trend to continue as more companies take advantage of the benefits of voluntary self-disclosure and the CEP more generally.

"The Criminal Division has successfully used whistleblower tips for years to open or advance white collar investigations. Our colleagues at the SEC, CFTC, and now at FinCEN have established programs, and we coordinate closely with them when whistleblowers provide tips that identify potentially criminal misconduct. This experience has positioned us well to help design DOJ's new pilot program.

Data Security Readiness

Assistant Attorney General **Matthew G. Olsen** used the ABA conference to discuss Justice's support of the White House's Executive Order on Data Security [11834], and the response he suggests companies and their counsel take.

"Now, the Department of Justice will do our part to make it harder for foreign adversaries to get their hands on this type of information. We are moving fast. One week in, I'll note three developments.

First, minutes after the President signed his Executive Order, I signed a 90-page **Advance Notice of Proposed Rulemaking**, or ANPRM, that kicks off the rulemaking process and seeks public comments to help us refine the program. [89 FR 15780]

Second, we are crafting a strategy for enforcement and compliance of this program. Just as we've done with sanctions and export controls, that strategy will have real teeth

Third, we are ramping up our staffing and resources significantly. This regulatory program will require us to bring on dozens of new attorneys and non-attorneys with expertise in general and specific licensing, targeting and designations, guidance and advisory opinions, and policy and regulatory development. We will also be substantially increasing FIRS's Compliance and Enforcement, and we've appointed a new Deputy Chief for National Security Data Risks.

Here is our advice to companies:

• **Know your data.** It is worth the investment to understand fully what categories of data you transact in and how much — and whether you have appropriate safeguards in place to ensure that sensitive information cannot be misused.

• **Know where that data is going:** You should review existing agreements to sell or provide your data to others — including advertisers, marketers, and vendors — and update those agreements now to ensure you have sufficient confidence in where that data is going.

• **Know who has access to the data:** The proposed rules would apply to certain transfers of data to non-U.S. consultants and investors who are based in countries of concern, including China, Russia, and Iran. That means you need to understand what data you are making available and to consider the implications.

• **Know your data sales:** Consider any transactions you have involving the sale of data, and consider whether you have confidence in the business practices of any third-party data brokers you deal with, directly or indirectly.

The answers here are not one-size-fits-all. As in the sanctions and export control regime, companies will need to develop risk-based compliance programs tailored to their individualized risk profiles. [11859]

BIS

Automatic EAR Restrictions for Sanctioned Parties

The Commerce Department's Bureau of Industry and Security (BIS) released a final rule to impose additional restrictions under the Export Administration Regulations (EAR) on persons identified under fourteen sanctions programs, on the List of Specially Designated Nationals and Blocked Persons (SDN List) maintained by the Department of the Treasury's Office of Foreign Assets Control (OFAC).

"Export controls and financial sanctions have long been complementary, and today's rule will serve as a force multiplier in their overall effectiveness," **said Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler.**"In the context of our response to Russia's horrific invasion of Ukraine, we have seen just how important close coordination in applying both export controls and financial sanctions is to undermine the ability of foreign adversaries to

Continues on next page

Continued from previous page

fund their destabilizing activities and obtain the items they seek to carry out those activities."

While the EAR has for many years restricted the export, reexport, and transfer (in-country) transactions involving certain persons and entities identified on the SDN List or pursuant to certain statutory authorities, **the new rule ensures that persons and entities blocked under fourteen OFAC sanctions programs will also automatically be subject to stringent export, reexport, and transfer (in-country) controls under the EAR.** The fourteen OFAC sanctions programs consist of:

• Seven Executive Orders related to Russia's harmful foreign activities, including its aggression in Ukraine dating back to its 2014 annexation of Crimea as well as the recent further invasion in 2022 and the undermining of democratic processes or institutions in Belarus;

• Two programs related to terrorism (Foreign Terrorist Organizations Sanctions Regulations and Global Terrorism Sanctions Regulations);

• The Weapons of Mass Destruction Proliferators Sanctions Regulations; and Four programs related to narcotics trafficking and other criminal networks

ADOBESTOCK / ANTON

Seven Executive Orders issued related to Russia's harmful foreign activities, including its aggression in Ukraine.

Because the EAR's restrictions focus primarily on the export of items, Commerce authorities can serve to complement OFAC's blocking measures targeting financial dealings, especially for transactions that involve items subject to the EAR but do not involve U.S. persons.

The rule also makes structural and technical changes to consolidate existing SDN-related EAR restrictions so that all SDN-related provisions are in the same section of Part 744 (Control Policy: End-User and End-Use Based), which describes the EAR's prohibitions against exports, reexports, and transfers (in-country) of items to certain end users and end uses unless authorized by BIS. [11929]

Estevez Pleads for Funds to Meet BIS Workload

Notwithstanding a doubled caseload, antiquated systems, and flat budget for the past ten years, the Commerce Department's Bureau of Industry and Security (BIS) has been keeping pace, Undersecretary for Industry and Security Alan Estevez told a congressional panel.

"BIS has been asked to do more in an era of strategic competition where economic statecraft is increasingly central to U.S. interests and strategy," he told the House Committee on Foreign Affairs March 21. "We have risen to every challenge that we have been asked to take on.

"However, to sustain our current pace and effectiveness, there are a few realities that the Committee should consider:

• BIS's budget for core export control functions has remained essentially flat since 2010, when adjusted for inflation.

• BIS' law enforcement arm, OEE, employs only 150 agents to counter the threat posed by nation state actors, which means an increase in sworn law enforcement officers and analysts is overdue.

• Total U.S. exports are up approximately 62 percent since 2010, and exports subject to BIS license requirements are up approximately 126 percent since 2014.

'BIS has been asked to do more in an era of strategic competition where economic statecraft is increasingly central to U.S. interests and strategy.'

Alan Estevez, Undersecretary for Industry and Security

• Our licensing workload has doubled from approximately 20,000 per year in 2012, to over 40,000 per year.

• Our staff are relying on foundational systems for both license adjudication and enforcement work that were put in service in 2006 and 2008, respectively.

• License review timelines continue to increase, particularly to the PRC, as licenses become more complex, particularly for exports of electronic components.

"Notwithstanding these challenges, we achieved an all-time high in the number of criminal convictions and months in jail, resolved or imposed the highest number of administrative cases, denial orders, and temporary denial orders, and conducted a record 1,500 end use checks globally in fiscal year 2023. " Mr. Estevez told the House Committee on Foreign Affairs.

The Whilte House's proposed budget earmarks $223 million for BIS, an increase from the $191 million of the past two years. By comparison, Lockheed Martin's F-35 Lightning II fighter jet costs the government around $109 million a copy.

Sector-Based Sanctions Over Entity List

"In China, I can't tell because of civil military fusion how those chips are going to be applied and we know that they are going to be applied to military applications.

"Establishing a technological cut line, and saying anything above this cut line should not be allowed in China because I can't tell its use case is way more effective. It's more effective for industry because they can understand where that line is, and they can then plan out what their business opportunities are.

"And it's more effective from my enforcement perspective. You know, sanctions, export controls, using the entity list is a whack-a- mole game where, to your point, people change and then we have to go after the next one, which we're happy to do. It's more strategic to go after a sector technological basis." [11931]

BRIEFS

BIS

October 25 Chip Rule Revision Published

➤ BIS has published corrections and amendments to the October 25 2023 Semiconductor and Advanced Computing Rules. This rule corrects inadvertent errors in those rules and makes additional clarifications for the two rules.

China has expressed strong opposition to the latest U.S. rules on semiconductor export rules, saying that it will disrupt the global semiconductor market as well as cooperation between enterprises.

On October 25, 2023, the Bureau of Industry and Security (BIS) published in the Federal Register the interim final rules (IFR), **"Export Controls on Semiconductor Manufacturing Items" (SME IFR) and "Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections"** (AC/S IFR).

ADOBESTOCK

Changes incorporated in the final rule include:

Revisions to § 740.8 Notified Advanced Computing (NAC) and Advanced Computing Authorized (ACA), with a particular emphasis on Macau-linked entities.

This rule also adds a new paragraph (a)(3) to clarify that for ECCNs 5A002.z, 5A004.z, or 5D002.z, all License Exception Encryption commodities, software, and technology (ENC) requirements under § 740.17 of the EAR must also be met for eligibility under License Exceptions NAC or ACA.

Revisions to § 744.23. This rule amends paragraph (c) of § 744.23 to state that License Exceptions in § 740.2(a)(9) (i) and (ii) of the EAR may overcome the license requirements imposed by § 744.23(a)(4) and (a)(3)(i) of the EAR,

Continues on next page

BRIEFS

respectively.

Revisions to § 744.6 Restrictions on specific activities of "U.S. persons." BIS is adding EUV masks (ECCN 3B001.j) and associated software and technology to the control in paragraph (c)(2)(iii) for SME, because it was unintentionally excluded from controls. EUV masks are required for lithography and lithography is a critical technology for advance- node IC production.

Restoring controls for ECCNs that contain .z paragraphs. This rule restores controls in the license requirement table of ECCNs 3A001, 3D001, 3E001, 4A003, 4A004, 4A005, 4D001, 4E001, 5A002, 5A004, 5D002, and 5E002, by removing the exceptions for .z paragraphs from the national security (NS), missile technology, nuclear proliferation, and/or crime control license requirement paragraphs.

• Maintaining the status quo for license exception eligibility for certain destinations

• Revisions to 3A001

• Revisions to ECCN 3D001.

• Revision to ECCN 3E001 license requirements and reasons for control.

• Addition of missing paragraph 4A090.b.

• Revisions to ECCN 4E001.

• Revisions to ECCN 5D002 and 5D992.

• Revisions to ECCN 5E992 and 5E002.

N. Revision to supplement no. 6 to part 774 — Sensitive List.

"Export Controls on Semiconductor Manufacturing Items" (SME IFR) (88 FR 73424, October 25, 2023)

• Corrections to ECCN 3B001 and 3B991. In ECCN 3B001, this rule corrects the scientific unit in paragraphs d.4.d.2 by replacing 13.33 kPa with 13.33 Pa; and in paragraph d.5 replacing 450 Mpa with 450 MPa.

• Revision of § 744.23(a)(4). BIS is revising the scope of the exceptions for masks in § 744.23(a)(4)(i), because it unintentionally excepted EUV masks in 3B001.j, as well as equipment in 3B991.b.2.

• Clarification to BIS responses to certain public comment topics. [11980]

Radiation Hardened Integrated Circuits and Expansion of License Exception GOV

➤ The Bureau of Industry and Security (BIS) is amending the Export Administration Regulations (EAR) to clarify controls on radiation hardened integrated circuits, including controls on computer and telecommunications equipment incorporating such radiation hardened integrated circuits.

This rule also addresses certain scenarios that apply to certain integrated circuits acquired, tested, or otherwise used by or for the United States Government and affirms the availability of License Exception GOV for such items when pursuant to an official written request or directive from the Department of Defense or the Department of Energy.

Lastly, this rule expands the availability of License Exception GOV for microelectronics items in order to remove export control obstacles for official business of the U.S. Government, including the Department of Energy and the Department of Defense. [89 FR 18353]

House Panel Zeroes in on China Biotech

The leaders of the House Select Committee on China are warning that a Chinese military company, BGI, is attempting to set up a new firm, Inomics, in Massachusetts and Kentucky, to avoid US regulatory scrutiny.

In a letter to Defense Secretary Lloyd Austin, Committee Chairman Mike Gallagher (R-Wisc) and ranking Democrat Raja Krishnamoorthi (Ill) urged the Pentagon to label Chinese companies that aid the Chinese Communist Party in military biotech research as "Chinese Military Companies."

"The PRC's 14th Five-Year Plan identifies dominance in biotechnology as critical to 'strengthen the PRC's science and technological power' and calls to deepen military-civil science and technology collaboration in the sector," the lawmakers wrote.

"PRC military and academic literature further stresses the importance of biotechnology to national power, arguing success on the future battlefield will require 'achieving biological dominance,' with one former president of the People's Liberation Army's (PLA) National Defense University openly discussing biotech's ability to create synthetic pathogens that are 'more toxic, more contagious, and more resistant.' Urgent action is needed to identify the PRC biotechnology entities at the forefront of this work."

In other Commitee News, they called on the Pentagon to consider labeling the following biotech companies 'Chinese Military Companies': MGI Group and Complete Genomics, Innomics and STOmics, Origincell, Vazyme Biotech and Axbio. Speaker Mike Johnson named Michigan representative John Molnar to take over the Chairmanship of the House Select Committee on the Chinese Communist Party being vacated by Rep. Mike Gallagher(R-WI).

The Midland Michigan lawmaker can be expected to continue Mr. Gallagher's efforts to cultivate bipartisan consensus on commercial relations with our greatest adversary. [12009]

Insiders Charged in Tesla Battery Tech Theft

A Canadian national was arrested in New York, for conspiring to send to undercover law enforcement officers trade secrets that belonged to his previous employer, Tesla Motors Canada subsidiary Hibar Systems Ltd. Klaus Pflugbeil and Yilong Shao allegedly used stolen confidential information — developed by Hibar — to establish their own Chinese-based competitor.

According to court documents, Pflugbeil and Shao are operators of a Hife Systems, Ltd., a PRC-based business that sold technology used for the manufacture of batteries, including batteries used in electric vehicles. The defendants built their business using Hibar's sensitive and proprietary information, and marketed their business as a replacement for Hibar's products.

Pflugbeil was arrested after he sent multiple trade secrets to an undercover agent and traveled to Nassau County for a meeting with who he believed to be Long Island-based businesspeople, but who in reality were undercover law enforcement agents.

In 2019, Tesla acquired Hibar Systems, a Canada-based manufacturer of automated, precision dispensing pumps and battery assembly lines. Prior to its purchase, the Canadian Manufacturer sold battery assembly lines to customers who manufactured alkaline and lithium-ion batteries for consumer use.

Both Pflugbeil and Shao are former employees of Hibar. According to his online profile, Pflugbeil spent 14 years with Hibar managing technology transfer and manufacturing in China,

The complaint alleges that, by no later than 2019, Pflugbeil and Shao planned to make use of Hibar trade secrets for their own business activities. For example, between October and November 2019, Pflugbeil and Shao discussed "set[ting] up" a company in Canada and China that would

Continues on next page

According to court documents, Pflugbeil and Shao are operators of a Hife Systems, Ltd

Continued from previous page

rely on the sensitive and confidential information needed to make and sell their own battery technology. Pflugbeil told Shao that he had "a lot of original documents" related to the technology and sought out more "original drawings" from Hibar that they could copy for their planned business. Shao subsequently confirmed that "we have all of original assembly drawings by PDF."

In or about July 2020, Pflugbeil and Shao opened Hife Systems, Ltd., which has since expanded to locations in China, Canada, Germany, and Brazil. Hife makes the same precision dispensing pumps and battery assembly lines that Hibar manufactured using its proprietary technology. Hife is marketed by Pflugbeil as an alternative source for the sale of products that rely upon Hibar trade secrets, publishing online advertisements that state, for example, "Are you looking for Hibar Metering pumps and spare parts? Look no further."

In December 2021, Tesla Totonto Automation entered into a license agreement with Japan's Unicontrols Co for "exclusive manufacturing and exclusive sales of the Hibar precision pump business. "

In operating Hife, Pflugbeil and Shao relied upon the Battery Assembly Trade Secret. For example, in September 2020, Pflugbeil emailed a series of drawings to a gears manufacturer in order to produce several parts and wrote "please keep the attached information confidential." The attachment contained drawings belonging to Hibar related to the Battery Assembly Trade Secret. The drawings that Pflugbeil sent were identical to Hibar drawings, except the name of the company was changed, the date of the drawing was changed, and the drawing identifying number was written in reverse of Hibar's drawing identifying number.

Undercover agents attended a trade show for the packaging and processing industries in Las Vegas, Nevada. The undercover agents posed as businesspeople who were interested in purchasing a battery assembly line to manufacture batteries at a facility on Long Island, New York. The undercover agents were introduced to Shao at the trade show and later to Pflugbeil via email.

Subsequently, on or about Nov. 17, 2023, Pflugbeil sent, via email, a detailed 66-page technical documentation proposal to an undercover agent. The proposal notes, "this technical documentation package contains proprietary information which must be kept confidential." In reality, the proposal contained Battery Assembly Trade Secret information belonging to Hibar: at least half a dozen drawings Pflugbeil used in the proposal and sent to UC-1 were, in fact, Hibar's information related to the Battery Assembly Trade Secret.

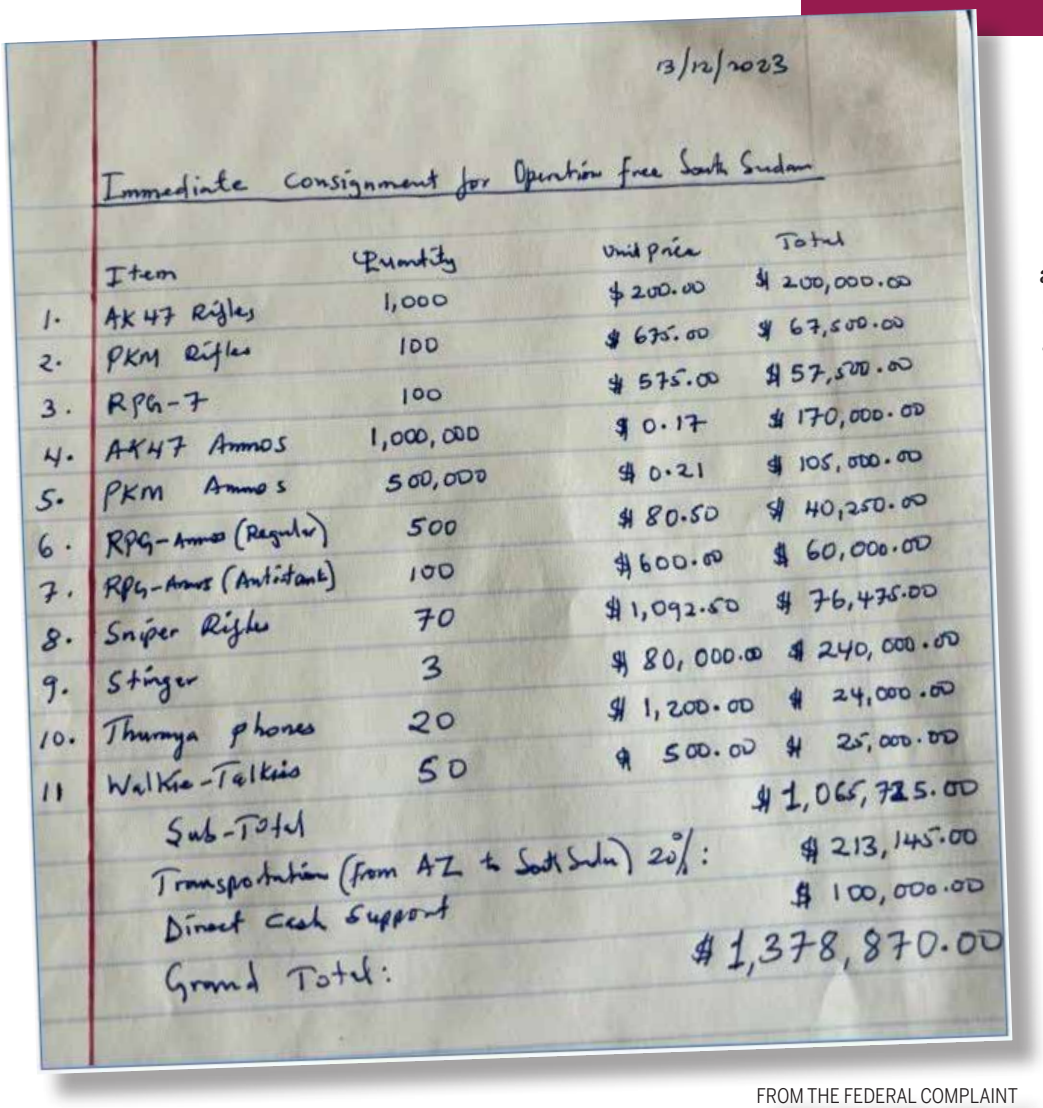
If convicted, Pfugbeil faces a maximum penalty of 10 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors. [11927]

South Sudan Coup Smugglers Foiled

A federal criminal complaint unsealed March 4th charges two men with conspiring to purchase and illegally export millions of dollars' worth of fully automatic rifles, grenade launchers, Stinger missile systems, hand grenades, sniper rifles, ammunition, and other export-controlled items from the United States to South Sudan, in violation of the Arms Export Control Act (AECA) and the Export Control Reform Act (ECRA).

One of the defendants **Peter Biar Ajak**, explained to the undercover agents that he was planning for "basically a coup ... with both internal and external fronts" against the current South Sudanese government, which he described as corrupt, illegitimate, and beholden to foreign interest groups.

He said he wanted to "knock it over and rebuild a new country," and that he would be installed as the new "Prime Minister" and "head of the government." He added his new government would be recognized by the United States and he "[has] the



13/12/2023

Immediate consignment for Operation free South Sudan

	Item	Quantity	Unit price	Total
1.	AK 47 Rifles	1,000	$ 200.00	$ 200,000.00
2.	PKM Rifles	100	$ 675.00	$ 67,500.00
3.	RPG-7	100	$ 575.00	$ 57,500.00
4.	AK47 Ammos	1,000,000	$ 0.17	$ 170,000.00
5.	PKM Ammos	500,000	$ 0.21	$ 105,000.00
6.	RPG-Ammo (Regular)	500	$ 80.50	$ 40,250.00
7.	RPG-Ammo (Antitank)	100	$ 600.00	$ 60,000.00
8.	Sniper Rifles	70	$ 1,092.50	$ 76,475.00
9.	Stinger	3	$ 80,000.00	$ 240,000.00
10.	Thuraya phones	20	$ 1,200.00	$ 24,000.00
11	Walkie-Talkies	50	$ 500.00	$ 25,000.00
	Sub-Total			$ 1,065,725.00
	Transportation (from AZ to South Sudan) 20%:			$ 213,145.00
	Direct Cash Support			$ 100,000.00
	Grand Total:			$ 1,378,870.00

FROM THE FEDERAL COMPLAINT

Defendant's shopping list.

backing of the State Department, implicitly."

Mr. Ajak a prominent figure in the South Sudanese diaspora, has been living in Maryland as an asylee and is a non-resident felow at the Harvard Kennedy School's Belfer Center.

In July 2018, in response to the conflict between South Sudan's Transitional Government of National Unity and opposition forces, the United Nations Security Council imposed an arms embargo on South Sudan. The Security Council has renewed the arms embargo every year since 2018, most recently in May 2023.

Under U.S. law, specifically the AECA and ECRA, it is unlawful to export weapons and ammunition to South Sudan absent authorization in the form of a license from the U.S. Department of State or the Department of Commerce. It is the policy of the United States to deny licenses and approvals to export to South Sudan defense articles.

Between at least February 2023 and February 2024, **Abraham Chol Keech** and Mr. Ajak sought to illegally purchase weapons and related export-controlled items from undercover law enforcement agents and smuggle those weapons and items from the United States to South Sudan through a third country.

The defendants knew that South Sudan was subject to an arms embargo and that exporting weapons and ammunition from the United States to South Sudan without a license from the U.S. government was illegal and would violate U.S. law.

For example, the defendants openly discussed the illegality of the transaction, expressed the need to be discreet, and agreed to pay a risk fee for the weapons because of the illegal nature of the arms sale. In addition, to facilitate the smuggling scheme, the defendants discussed disguising the weapons as humanitarian aid and paying bribes.

As part of the scheme, the defendants further sought to conceal from financial institutions and others the source and purpose of the funds used to purchase and smuggle the illicit arms.

For example, the defendants agreed to an arms contract for nearly $4 million worth of weapons and related items and requested a "fake contract" in the same amount in "consulting services" and items, such as "communications equipment," related to "human rights, humanitarian, and civil engagement inside South Sudan refugee camps." The defendants then caused funds to be transferred through an intermediary company identified in the fake contract to complete the purchase.

If convicted, the defendants face up to 20 years in prison for conspiring to violate the AECA, up to 20 years in prison for conspiring to violate the ECRA, and up to 10 years in prison for smuggling goods from the United States. [11878]

Google Engineer Steals AI IP for Chinese Venture

A federal grand jury has indicted a Chinese national, charging him with four counts of theft of trade secrets in connection with an alleged plan to steal from Google proprietary information related to artificial intelligence (AI) technology.

According to the indictment **Linwei Ding**, 38, a national of the PRC and resident of Newark, California, transferred sensitive Google trade secrets and other confidential information from Google's network to his personal account while secretly affiliating himself with PRC-based companies in the AI industry. Ding was arrested March 6th.

"While we work to responsibly harness the benefits of AI, the Justice Department is on high alert to its risks, including global threats to our national security," said **Deputy Attorney General Lisa Monaco**. "As alleged in today's charges, the defendant stole from Google over 500 confidential files containing AI trade secrets, while covertly working for China-based companies seeking an edge in the AI technology race. The Justice Department will relentlessly pursue and hold accountable those who would siphon disruptive technologies — especially AI — for unlawful export."

SHAWN COLLINS (CC BY 2.0)

According to court documents, the technology Ding allegedly stole involves the building blocks of Google's advanced supercomputing data centers, which are designed to support machine learning workloads used to train and host large AI models, applications capable of understanding nuanced language and generating intelligent responses to prompts, tasks, or queries.

The indictment describes how Google developed both proprietary hardware and software to facilitate the machine learning process powered by its supercomputing data centers. The firm uses advanced computer chips with the extraordinary processing power required to facilitate machine learning and run AI applications. Google deploys several layers of software, referred to in the indictment as the "software platform," to orchestrate machine learning workloads efficiently.

Google hired Ding as a software engineer in 2019. His responsibilities included developing the software deployed in Google's supercomputing data centers. In connection with his employment, Ding was granted access to Goggle's confidential information related to the hardware infrastructure, the software platform, and the AI models and applications they supported.

On May 21, 2022, Ding began secretly uploading trade secrets that were stored in Google's network by copying the information into a personal Google Cloud account. Ding continued periodic uploads until May 2, 2023, by which time Ding allegedly uploaded more than 500 unique files containing confidential information.

In addition, the indictment alleges that Ding secretly affiliated himself with two PRC-based technology companies. According to the indictment, on or about June 13, 2022, Ding received several emails from the CEO of an early-stage technology company based in the PRC indicating Ding had been offered the position of Chief Technology Officer for the company.

Ding allegedly traveled to the PRC on Oct.

29, 2022, and remained there until March 25, 2023, during which time he participated in investor meetings to raise capital for the new company. The indictment alleges potential investors were told Ding was the new company's Chief Technology Officer and that Ding owned 20% of the company's stock.

Unbeknownst to Google, by no later than May 30, 2023, Ding had founded his own technology company in the AI and machine learning industry and was acting as the company's CEO. Ding's company touted the development of a software platform designed to accelerate machine learning workloads, including training large AI models.

Ding applied to a PRC-based startup incubation program and traveled to Beijing, to present his company at an investor conference on Nov. 24, 2023. A document related to Ding's startup company stated, "we have experience with Google's ten-thousand-card computational power platform; we just need to replicate and upgrade it — and then further develop a computational power platform suited to China's national conditions."

The indictment describes measures that Ding allegedly took to conceal his theft of the trade secrets. For example, he allegedly copied data from Google source files into the Apple Notes application on his Google-issued MacBook laptop. By then converting the Apple Notes into PDF files and uploading them from the Google network into as separate account, Ding allegedly evaded detection by Google's data loss prevention systems.

Likewise, the indictment describes how in December 2023 Ding allegedly permitted another Google employee to use his Google-issued access badge to scan into the entrance of a Google building — making it appear he was working from his U.S. Google office when, in fact, he was in the PRC.

Ding is charged with four counts of theft of trade secrets. If convicted, Ding faces a maximum penalty of 10 years in prison and up to a $250,000 fine for each count. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors. [11854]

Yet Another Swiss Trader Fined in Petrobras Graft

Swiss commodity broker Trafigura pleaded guilty to crimes related to bribing Brazilian officials of the state owned oil company Petrobras, the Justice Department announced March 28.

The $126 million settlement noted the firm's extensive prior misconduct, as well that "Trafigura was slow to exercise disciplinary and remedial measures, " and "Trafigura failed to preserve and produce certain documents and evidence in a timely manner and, at times, took positions that were inconsistent with full cooperation."

Trafigura Beheer B.V. pleaded guilty to resolve an investigation by the U.S. Justice Department into violations of the Foreign Corrupt Practices Act (FCPA), stemming from the company's corrupt scheme to pay bribes to Brazilian government officials to secure business with Brazil's state-owned and state-controlled oil company, Petróleo Brasileiro S.A. — Petrobras.

Trafigura pleaded guilty to conspiracy to violate the anti-bribery provisions of the FCPA. Pursuant to the plea agreement, Trafigura will pay a criminal fine of $80,488,040 and forfeiture of $46,510,257. The department will credit up to $26,829,346 of the criminal fine against amounts Trafigura pays to resolve an investigation by law enforcement authorities in Brazil for related conduct. Trafigura reported $7.4 billion in profits in 2023, nearly 59 times the criminal penalty.

"For more than a decade, Trafigura bribed Brazilian officials to illegally obtain business and reap over $61 million in profits," said **Principal Deputy Assistant Attorney General Nicole M. Argentieri**, head of the Justice Department's Criminal Division. "Today's guilty plea underscores that when companies pay bribes and undermine the rule of law, they will face significant penalties. The department remains determined to combat foreign bribery and hold accountable those who violate the law."

According to court documents, between approximately 2003 and 2014, Trafigura and its co-conspirators paid bribes to Petrobras officials in order to obtain and retain business with

Continues on next page

Trafigura profited approximately $61 million from the corrupt scheme.

TRAFIGURA PHOTO

Petrobras. Beginning in 2009, Trafigura and its co-conspirators, who met in Miami to discuss the bribery scheme, agreed to make bribe payments of up to 20 cents per barrel of oil products bought from or sold to Petrobras by Trafigura and to conceal the bribe payments through the use of shell companies, and by funneling payments through intermediaries who used offshore bank accounts to deliver cash to officials in Brazil. Trafigura profited approximately $61 million from the corrupt scheme.

The department reached this resolution with Trafigura based on a number of factors, including, among others, the nature and seriousness of the offense.

Trafigura received credit for its cooperation with the department's investigation and affirmative acceptance of responsibility, which included

• providing timely updates on facts learned during its internal investigation;

• making factual presentations to the department;

• facilitating the interviews of employees and agents, including an employee located outside the United States, and arranging for counsel for employees where appropriate;

• producing relevant non-privileged documents and data to the department, including documents located outside the United States in ways that navigated foreign data privacy laws, accompanied by translations of certain documents; and

• providing all relevant facts known to it, including information about individuals involved in the conduct.

"However, and particularly during the early phase of the department's investigation, Trafigura failed to preserve and produce certain documents and evidence in a timely manner and, at times, took positions that were inconsistent with full cooperation," the Justice Department said.

Trafigura also engaged in remedial measures, including:

• developing and implementing enhanced, risk-based policies and procedures relating to, among other things, anti-corruption, use of intermediaries and consultants, third party payments, and joint venture and equity investment risk assessment;

• enhancing processes and controls around high-risk transactions;

• investment of additional resources in employee training and compliance testing; (iv) enhancing ongoing compliance monitoring and controls testing processes; and

• proactively discontinuing the use of third-party agents for business origination.

However, Trafigura was slow to exercise disciplinary and remedial measures for certain employees whose con-

duct violated company policy.

In addition, Trafigura's prior misconduct, though not recent, includes a 2006 guilty plea by Trafigura AG for entry of goods by means of false statements; as well as Trafigura's 2010 conviction of violating Netherlands export and environmental laws in connection with the discharge of petroleum waste in Côte d'Ivoire.

While Trafigura ultimately accepted responsibility for its criminal conduct in this investigation, its early posture in resolution negotiations also caused significant delays and required the department to expend substantial efforts and resources to develop additional admissible evidence before

Trafigura constructively reengaged in agreeing to a negotiated resolution. Accordingly, the department determined that the appropriate resolution in this case was for Trafigura to plead guilty to one count of conspiracy to violate the FCPA.

$13 million discount

The criminal fine calculated under the U.S. Sentencing Guidelines reflects a 10% reduction off the fifth percentile of the applicable guidelines fine range, which accounts for Trafigura's cooperation and remediation, as well as its prior history.

Angola, Exim Involvement

Trafigura is reportedly facing a separate investigation by Swiss authorities into senior executive's involvement in bribery in Angola, and has been under investigation by the CFTC for commodity price manipulation. Angola booster and globetrotting president of the US Export Import Bank **Reta Jo Lewis** announced last summer a guarantee for a $400 million credit facility for Trafiguras Liquified Natural Gas trading book. [10752]

Jeremy Weir, Executive Chairman and CEO of Trafigura said in a statement: "These historical incidents do not reflect Trafigura's values nor the conduct we expect from every employee. They are particularly disappointing given our sustained efforts over many years to embed a culture of responsible conduct at Trafigura."

'Trafigura failed to preserve and produce certain documents and evidence in a timely manner and, at times, took positions that were inconsistent with full cooperation.'

Commodity Firms: 20 Convictions, $1.7 Billion in Fines

The Global commodity trading community has long been a honey pot for corrupt officials and rogue operators. Many firms, including **Glencore** and **Trafigura** trace their lineage back to the notorious fugitive "King of Oil" **Marc Rich**.

Rich fled the United States in 1983 when indicted on charges of tax evasion, fraud, racketeering and illegal trading of oil with Iran. He was later pardoned by **President Bill Clinton** after Rich's former wife Denise gave the Clinton Library $450,000. Rich died in Switzerland in 2013.

The Justice Department investigation into international commodities trading companies that paid bribes to win business with state-owned and state-controlled oil companies in Latin America and Africa has resulted in six corporate resolutions, 20 convictions of individuals, and total fines, forfeitures, and other penalties of more than $1.7 billion.

Since 2017, the Criminal Division's Fraud Section's Foreign Corrupt Practices Act (FCPA) Unit, in partnership with U.S. Attorneys' Offices across the country, the Money Laundering and Asset Recovery Section, and the FBI, has been investigating corruption committed by international commodities trading companies, which paid millions of dollars in bribes to corrupt government officials to secure billions of dollars in business with state-owned enterprises.

Through this work, the Criminal Division has entered into six corporate resolutions, which have included mandatory cooperation, disclosure, and compliance obligations and resulted in total fines, forfeitures, and other penalties of more than $1.7 billion:

• In September 2020, Sargeant Marine Inc., an

Continues on next page

Continued from previous page

asphalt company based in Boca Raton, Florida, with an asphalt trading arm, pleaded guilty in the Eastern District of New York to schemes to bribe government officials in Brazil, Venezuela, and Ecuador;

• In December 2020, Vitol Inc., entered into a deferred prosecution agreement (DPA) in the Eastern District of New York, admitting to schemes to pay bribes to government officials in Brazil, Ecuador, and Mexico;

• In May 2022, Glencore International AG pleaded guilty in the Southern District of New York to a scheme to pay bribes to government officials in seven countries across Africa and Latin America;

• In December 2023, Freepoint Commodities LLC entered into a DPA in the District of Connecticut and admitted to a scheme to bribe government officials in Brazil;

• In March, Gunvor S.A. pleaded guilty in the Eastern District of New York to a scheme to bribe government officials in Ecuador; and

• Also in March, Trafigura Beheer B.V. pleaded guilty in the Southern District of Florida to a scheme to bribe government officials in Brazil. [11969]

BRIEFS

Ericsson Ethics and Compliance Makeover Continues

➤ Beleaguered Swedish telecoms maker Ericsson has shaken up its compliance operation once again, naming **Becky Rohr**, current head of investigations, head of compliance as well. Jan Sprafke, appointed compliance chief six months ago, will be leaving the company.

Ms. Rohr was previously Vice President, Anti-Corruption and Global Trade, Ethics & Compliance Office at Hewlett Packard, and held numerous roles in civil and criminal fraud prosecution in the Justice Department. She will keep her office in Washington, DC.

Last March the company signed a deal with the Justice Department cknowledging breaches of the deferred prosecution agreement it entered into for corruption in Djibouti, China, Vietnam, Indonesia and Kuwait, as well as failure to report and disclose an illicit alliance with the Islamic State in Iraq uncovered by press reports in 2022.

Ericsson entered a guilty plea regarding previously deferred charges relating to conduct prior to 2017. The plea agreement called for $207 million in additional fines and an extension of the independent compliance monitor until June 2024. In 2013 Ericsson disclosed that it was cooperating with U.S. authorities investigating bribery allegations, resulting in a $1 billion bribery settlement in 2019. That settlement contained no mention of Iraq. [11851]

Latvian Indicted in Honeywell Avionics Scheme

➤ The Latvian partner of a Kansas avionics distributor has been indicted for his role in a years-long scheme to sell sophisticated avionics equipment to Russian companies, in violation of U.S. export laws. The defendant is the third to be arrested and charged in connection with the conspiracy led by a Kansas company and two U.S. nationals, originally reported on March of 2023 [9505]

Oleg Chistyakov, 55, was arrested on March 19 near Riga, Latvia, and remains detained pending extradition proceedings. His Kansas-based co-conspirators were arrested in March 2023 [9505]

According to court documents, after Russia's invasion of Ukraine in February 2022 and despite additional U.S. economic countermeasures levied against Russia, Chistyakov and his conspirators continued to smuggle and export sophisticated and controlled avionics equipment to companies in Russia without the required licenses from the U.S. Department of Commerce.

Chistyakov, operating from Latvia, worked with his conspirators through their U.S. company, KanRus Trading Company Inc., a Honeywell (Bendix-King) distributor, purchasing avionics equipment from U.S. companies for customers in Russia. Actions allegedly taken by Chistyakov and his conspirators to conceal their illegal activities included creating false invoices, transshipping items through third-party countries, using bank accounts in third-party countries, and exporting items to intermediary companies which then reexported the items to the ultimate end destinations.

Chistyakov faces a maximum penalty of five years in prison for conspiracy, 20 years in prison for each Export Control count, 10 years in prison for each smuggling count and 20 years in prison for each money laundering count. [11968]

California Man Sentenced for Arms to Oman

➤ A California man was sentenced for attempting to ship firearms and night-vision equipment to the Sultanate of Oman. Fares Abdo Al Eyani, 41, was

sentenced to 12 months and a day in prison, followed by three years of supervised release, for conspiring to export defense articles and attempting to export defense articles.

According to court documents, Al Eyani acquired no less than four firearms with magazines and ammunition, and at least 44 rifle scopes, monoculars, and goggles with night vision capabilities in 2019. In November and December of that year, Al Eyani attempted to send the firearms and optics to the Sultanate of Oman in shipping containers departing from the Port of Oakland.

He concealed the firearms by disassembling them, wrapping them in aluminum foil, and then secreting them within automobiles inside the shipping container. Law enforcement searched the containers and seized the firearms, magazines, and ammunition, as well as the 44 rifle scopes, monoculars, and goggles with night vision capabilities, thereby thwarting Al Eyani's unlawful scheme.

The items Al Eyani attempted to export — four firearms, magazines, ammunition, and night-vision rifle scopes — were defense articles prohibited from export without a license by the AECA and the ITAR. Al Eyani did not have a license to export the defense articles. [11985]

Stericycle Executive Charged

➤ A federal grand jury in the Southern District of Florida returned an indictment March 18 charging a former finance director of the Latin America division of Stericycle Inc., an international waste management company headquartered in Lake Forest, Illinois, for his role in an alleged scheme to pay over $10 million in bribes to foreign officials in Brazil, Mexico, and Argentina.

According to court documents, between 2011 and 2016, **Abraham Cigarroa Cervantes**, 51, of Mexico, and others caused hundreds of bribe payments to be made to government officials in Brazil, Mexico, and Argentina to obtain and retain business and to secure improper advantages for Stericycle. A fellow executive in firm's Latin American operations, **Mauricio Gomez Baez** was indicted and entered into a plea agreement in February. These indictments are unusual in that they name persons employed by the offending company.

Employees at Stericycle's offices in Mexico, Brazil, and Argentina allegedly made bribe payments, typically in cash, to officials at government customers.

To conceal the payments, Cigarroa and others maintained false books, records, and accounts that did not accurately and fairly reflect the transactions and dispositions of Stericycle's assets, causing Stericycle to falsely record bribe payments as legitimate expenses in its consolidated books, records, and accounts. Cigarroa also allegedly submitted and maintained falsified Sarbanes-Oxley certifications and business unit representation letters falsely attesting that the books, records, and accounts were accurate.

STERICYCLE

To read complete articles, click on the Story ID number.

Cigarroa is charged with one count of conspiracy to violate the Foreign Corrupt Practices Act's (FCPA) anti-bribery provisions and one count of conspiracy to violate the FCPA's books and records provisions. If convicted, he faces a maximum penalty of five years in prison on each count.

In April 2022, Stericycle admitted to bribing officials in Mexico, Brazil, and Argentina in violation of the FCPA's anti-bribery and books and records provisions. Stericycle entered into a three-year deferred prosecution agreement with the Criminal Division's Fraud Section and agreed to pay more than $84 million as part of a coordinated resolution with the Justice Department, the Securities and Exchange Commission, and authorities in Brazil. [11928]

Fashion Brand Customs Fraud: Four Years Prison and $10.4 million

➤ A California fashion company executive was sentenced today to 48 months in federal prison for undervaluing imported garments in a scheme to avoid paying millions of dollars in customs duties. **Mohamed Ghacham**, 40, was sentenced by United States District Judge Maame Ewusi-Mensah Frimpong, who also ordered him to pay $6,390,781 in

Continues on next page

FORD OTOSAN

Ford has been building Transit Vans in Turkey since 1967

BRIEFS

Continued from previous page

restitution. Ghacham pleaded guilty in December 2022 to one count of conspiracy to pass false and fraudulent papers through a customhouse.

Mr. Ghacham's company, **Ghacham Inc.**, which does business under the "**Platini**" brand name, imported clothing from China and submitted fraudulent invoices to U.S. Customs and Border Protection (CBP) that undervalued the shipments, allowing the company to avoid paying the full amounts of tariffs owed on the imports. In December 2023, Judge Frimpong fined Ghacham Inc. $4 million, ordered it to pay $6,390,781 in restitution, and placed it on probation for five years.

Platini Jeans.
GHACHAM, INC.

At Mr. Ghacham's direction, Chinese suppliers would prepare two invoices for the clothing ordered by Ghacham Inc. — a true invoice, which reflected the actual price paid for the goods, and a fraudulent "customs invoice," which reflected an understated price. Ghacham Inc. submitted the customs invoices to CBP and customs brokers to fraudulently reduce the tariffs owed on the imports, while it maintained the true invoices in its accounting records.

From July 2011 to February 2021, Ghacham Inc. and Mohamed Ghacham undervalued imported garments by more than $32 million and failed to pay approximately $6,390,792 in customs duties.

Ghacham Inc. pleaded guilty in December 2022 to one count of conspiracy to pass false and fraudulent papers through a customhouse and one count of conspiracy to engage in any transaction or dealing in properties of a specially designated narcotics trafficker under a statute known as the Foreign Narcotics Kingpin Designation. [11862]

Ford Motor agrees to pay $365 million

In another Customs enforcement, **Ford Motor** agreed to pay the United States $365 million to resolve allegations that it violated the Tariff Act of 1930 by misclassifying and understating the value of hundreds of thousands of its Transit Connect vehicles. While the lost duties exceeded $183 million, no executives were targeted in the enforcement. The settlement resolves allegations that Ford devised a scheme to avoid higher duties by misclassifying cargo vans with "sham seats," evading the 25% "Chicken Tax" on light truck imports. [11904]

OFAC

Magnitsky Act Regs Expanded, Uyghur Act Incorporated

OFAC is amending and reissuing the Global Magnitsky Sanctions Regulations as a more comprehensive set of regulations that includes additional interpretive guidance and definitions, general licenses, and other regulatory provisions that will provide further guidance to the public.

As well, OFAC is adding the Uyghur Human Rights Policy Act of 2020, as amended. Due to the number of regulatory sections being updated or added, OFAC is reissuing the Regulations in their entirety.

The Regulations were initially issued in abbreviated form (in 2018) for the purpose of providing immediate guidance to the public. OFAC is revising the Regulations to further implement the Global Magnitsky Act and E.O. 13818.

Current Regulatory Action

To further implement the Global Magnitsky Act and E.O. 13818, OFAC is amending and reissuing the Regulations. The Regulations implement targeted sanctions that are directed at persons determined to meet the criteria set forth in § 583.201(a) of the Regulations, as well as sanctions that may be set forth in any further Executive orders issued pursuant to the national emergency declared in E.O. 13818.

The sanctions in E.O. 13818 do not generally prohibit trade or the provision of banking or other financial services to a certain country. Instead, the sanctions in E.O. 13818 apply where the transaction or service in question involves property or interests in property that are blocked pursuant to these authorities.

The names of persons designated or identified as blocked pursuant to E.O. 13818, or any further Executive orders issued pursuant to the national emergency declared therein, are published on OFAC's SDN List, which is accessible via OFAC's website. Those names also are published in the Federal Register as they are added to the SDN List. [11885]

BRIEFS

Nicaragua Trade Rules Tightened

➤ BIS amends the Export Administration Regulations (EAR) to apply more restrictive treatment to exports and reexports to, and transfers (in-country) within, Nicaragua of items subject to the EAR.

This action is consistent with the State Department's addition of Nicaragua to the list of countries that are subject to a U.S. arms embargo under the International Traffic in Arms Regulations (ITAR),

The State Department is adding Nicaragua to ITAR § 126.1 in paragraph (p). The policy of denial toward Nicaragua applies to licenses or other approvals for exports and imports of defense articles or defense services, except that a license or other approval may be issued on a case-by-case basis for non-lethal military equipment intended solely for humanitarian assistance, to include natural disaster relief.

Further, in accordance with ITAR § 129.7, no broker, as described in ITAR § 129.2, may engage in or make a proposal to engage in brokering activities subject to the ITAR that involve Nicaragua without obtaining the approval of the Directorate of Defense Trade Controls. Consistent with ITAR § 129.7(d), the Department of State will apply the same policy of denial to such requests.

To reflect this changed status under the ITAR, BIS adds Nicaragua to Country Group D:5. BIS's amendments also address concerns regarding the Nicaraguan Government's commission of human

Continues on next page

OFAC has sanctioned Wendy Carolina Morales Urbina, Nicaragua's Attorney General.
UNITED NATIONS TV

Continued from previous page

rights abuses against citizens and civil society groups, as well as the regime's ongoing military and security cooperation with Russia.

Specifically, BIS is moving Nicaragua from Country Group B to Country Group D, a more restrictive country grouping, applying a stringent licensing policy for items controlled for national security reasons, and making the country subject to 'military end use' and 'military end user' restrictions.

This rule advances the U.S. Government's efforts to restrict the availability of items subject to the EAR to Nicaragua's military and security services. [11897]

Nicaraguan AG Sanctioned

➤ Treasury's Office of Foreign Assets Control (OFAC) has sanctioned **Wendy Carolina Morales Urbina**, Nicaragua's Attorney General, for being complicit in the Ortega-Murillo regime's oppression.

"The Attorney General of Nicaragua, in concert with the Ortega-Murillo regime, has exploited her office to facilitate a coordinated campaign to suppress dissent by seizing property from government political opponents without a legal basis," said Under Secretary of the Treasury for Terrorism and Financial Intelligence, Brian Nelson.

In 2018, anti-government protests erupted in Nicaragua, prompting ongoing violent repression by the Ortega-Murillo regime. President Ortega and the Vice President, Rosario Murillo, Ortega's wife, have consolidated power, suppressed popular protests, incarcerated political opponents, and silenced critical voices in the media or forced them into exile.

On February 9, 2023, President Ortega expelled 222 political prisoners and put them on a flight to Washington, D.C. According to the Nicaraguan government, the deportation of the prisoners was intended to protect peace and national security and those freed have been declared traitors who can never serve in Nicaraguan public office. As a result, Nicaragua stripped the 222 former political prisoners of their Nicaraguan citizenship.

Ms. Morales Urbina is a Nicaraguan national who was appointed to the role of Attorney General of the Republic of Nicaragua in 2019, by President Ortega.

In her capacity as Attorney General, Morales Urbina is responsible for enabling the Ortega-Murillo regime to confiscate real property formerly belonging to independent media outlets, international organizations, and political prisoners.

In several instances Morales Urbina appeared in her official capacity in various private buildings, presented deeds to new owners and declared the properties were now being made for public use. Morales Urbina has also seized property from thousands of non-governmental organizations under law explicitly to suppress freedom of association.

Morales Urbina carried out the dispossession of all properties of the 222 political prisoners who were banished from Nicaragua. As well, she was key to formulating the strategy to designate Nicaraguan opposition members as terrorists and block their financial resources using an existing anti-terrorism law. [11938]

Russian Fake News Execs Sanctioned

➤ OFAC designated two individuals and two entities for services they provided the Government of the Russian Federation (GoR) in connection with a foreign malign influence campaign, including attempting to impersonate legitimate media outlets.

Nikolai Tupikin and **Ilya Gambashidze** were involved in a persistent foreign malign influence campaign at the direction of the Russian Presidential Administration. **SDA** and **Structura** have been identified as key actors of the campaign, responsible for providing GoR with a variety of services, including the creation of websites designed to impersonate government organizations and legitimate media outlets in Europe.

Leading into Fall 2022, **Tupikin** and **Gambashidze** implemented a campaign that impersonated news websites, staged videos, and fake social media accounts. Specifically, via their companies, **SDA** and **Structura**, the two created a sprawling network of over 60 websites that impersonated legitimate news organizations, and which used misleading social media accounts to amplify the content of the spoofed websites.

The fake websites appeared to have been built

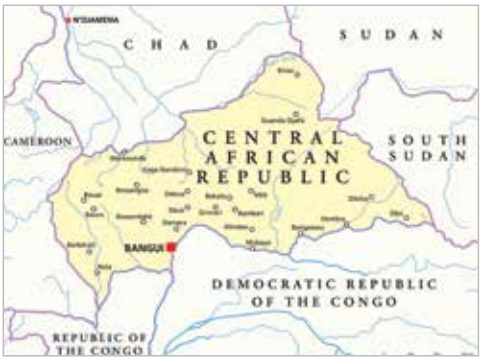
to carefully mimic the appearance of legitimate news websites. The fake websites included embedded images and working links to legitimate sites and even used the impersonated site's cookie acceptance page. [11941]

Wagner Group Sanctions in Africa

➤ OFAC sanctioned two companies — one in Russia and one in the Central African Republic (CAR) — for their efforts in advancing Russia's malign activities in CAR.

The March 8 action targets the operations of Private Military Company 'Wagner' (Wagner Group) and, by extension, the activities of the Russian Federation.

Those designated sought monetary gain from illicit natural resource extraction and provided material and financial support to the Wagner Group and other organizations associated with the enterprise of Yevgeniy Prigozhin, the former Wagner Group owner who died in August 2023 in a plane explosion in Russia.



"Russia has sought to leverage these Wagner-affiliated companies in its efforts both to secure additional revenue from abroad and to advance its interests in Africa, often at the expense of the host countries, their institutions, and their citizens," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.

"The United States remains focused on disrupting the networks that enable Russia's illicit and destabilizing activities in Africa."

Prigozhin Enterprise Companies

➤ **Bois Rouge SARLU** (Bois Rouge), a.k.a. Wood International Group SARLU, is a Bangui, CAR-based timber company., Bois Rouge received a natural resources concession in exchange for the services the Wagner Group provided in CAR. Bois Rouge acquired a timber permit in early 2021 around the same time Wagner Group mercenaries, in conjunction with CAR military forces, seized control of the corresponding area from rebels opposed to the CAR government. This land is in CAR's Lobaye prefecture, which is part of the Congo Basin and contains some of the largest undeveloped tracks of rainforest in the world. Bois Rouge has since exported tropical timber species, such as azobe, iroko, mukulungu, sapeli, and tali, to buyers in China, the Middle East, Europe, and Central Asia. In 2022, Bois Rouge's name changed to Wood International Group SARLU.

Limited Liability Company Broker Expert (Broker Expert) is a St. Petersburg, Russia-based company with a lengthy track record of supporting Prigozhin's exploits throughout Africa. Broker Expert has exported goods to several Prigozhin-associated companies, including dozens of shipments to Bois Rouge in CAR, multipurpose vehicles to U.S.-designated Meroe Gold Co. LTD. in Sudan, and helmets to Wagner Group forces in Ukraine. Moreover, Prigozhin's enterprise had used Broker Expert, among other companies, to regularly move cash to fund malign activities. For example, in Madagascar, a Prigozhin-associated company involved in a joint mining venture with a Malagasy state-owned enterprise received funds from Broker Expert.

The Wagner Group

➤ The United States has sanctioned numerous entities and individuals globally that support the Wagner Group and other Russian private military companies. The Wagner Group has committed widespread human rights abuses and has appropriated natural resources across multiple countries in Africa. A proxy military force of the Kremlin, the Wagner Group has carried out combat operations around the world, including in Russia's brutal war in Ukraine. Wagner has also participated in a scheme to procure weapons for its operations in Ukraine, using false end-use certificates in Mali.[11873]

Iran Suppliers Targeted

➤ OFAC targeted three procurement networks — based in Iran, Türkiye, Oman, and Germany — that have supported Iran's ballistic missile, nuclear, and defense programs. These networks have procured carbon fiber, epoxy resins, and other missile-applicable goods for Iran's arms proliferation activities.

Clients of the networks include Islamic Revolutionary Guard Corps Aerospace Force Self Sufficiency Jihad Organization, Ministry of Defense and Armed Forces Logistics, other U.S.-designated entities in Iran's defense industrial base, and Iran Centrifuge Technology Company, which is linked to the Atomic Energy Organization of Iran.

Action was taken pursuant to Executive Order (E.O.) 13382, which targets proliferators of weapons of mass destruction (WMD) and their means of delivery.

This action builds on OFAC's June 6, 2023 and October 18, 2023 designations targeting third-country procurement networks supporting the IRGC, MODAFL, and their subsidiaries' ballistic missile production. [11947]

Houthi Vessels & Shippers

➤ OFAC took additional action to target shipments of Iranian commodities undertaken by the network of Iran-based, Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF)-backed Houthi financial facilitator Sa'id al-Jamal.

The most recent action targets two Hong Kong- and Marshall Islands-based ship owners and two vessels for their role in shipping commodities on behalf of al-Jamal, and follows a February 27 action targeting a related vessel, the ARTURA.

Continues on next page

Continued from previous page

The revenue generated through al-Jamal's network continues to enable Houthi militant efforts, including ongoing and unprecedented attacks on international maritime commerce in the Red Sea and Gulf of Aden.

"The IRGC-QF and the Houthis continue to rely on the illicit sale of commodities to finance their attacks on commercial shipping in the Red Sea and Gulf of Aden," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "The United States remains resolved to hold accountable those who enable these destabilizing activities."

Irgc-Qf And Houthi Commodities Shipments

➤ Palau-flagged **RENEEZ**, which is owned and managed by Marshall Islands-based **Reneez Shipping Limited**, has transported tens of thousands of metric tons of Iranian commodities for the network of Iran-based IRGC-QF-backed Houthi financier Sa'id al-Jamal. Al-Jamal's network often uses falsified cargo documents to mask the Iran-origin cargo onboard and to obfuscate its ties to Iran and al-Jamal's network.

Reneez Shipping Limited is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Sa'id al-Jamal. The RENEEZ is being identified as blocked property in which Reneez Shipping Limited has an interest.

The Panama-flagged ARTURA was sanctioned as part of the February 27, 2024 action for transporting Iranian commodities on behalf of al-Jamal. ARTURA falsified its Automatic Identification System (AIS) to indicate it was traveling north from Singapore while the vessel was in the process of conducting a ship-to-ship (STS) transfer with the Panama-flagged **ETERNAL FORTUNE**. ETERNAL FORTUNE, which is owned by Hong Kong-based **Hongkong Unitop Group Ltd**, also emitted a false AIS signal while receiving the STS transfer from the ARTURA.

Hongkong Unitop Group Ltd is being designated pursuant to E.O. 13224, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Sa'id al-Jamal. The ETERNAL FORTUNE is being identified as blocked property in which Hongkong Unitop Group Ltd has an interest. [11880]

AMISOM

Mogadishu Fishing Harbor

Somali Sanctions: al-Shabaab

➤ The United States is designating sixteen entities and individuals in a transnational network that spans the Horn of Africa, United Arab Emirates, and Cyprus, for facilitating financing and money laundering for the al-Shabaab terrorist organization, a terrorist group responsible for some of the worst terrorist attacks in East Africa's modern history.

Al-Shabaab generates over $100 million per year by extorting local businesses and individuals, as well as through the financial support of affiliated businesspeople.

"The threat posed by al-Shabaab is not limited to Somalia. Al-Shabaab's revenues are disbursed to other al-Qa'ida-linked groups worldwide and help fund al-Qa'ida's global ambitions to commit acts of terrorism and undermine good governance,"said **State Department Spokesperson Matthew Miller**. [11915]

Zimbabwe Sanctions get More Personal

➤ Treasury is designating three entities and eleven individuals, including **President Emmerson Mnangagwa**, pursuant to Executive Order 13818, which builds upon and implements the Global Magnitsky Human Rights Accountability Act, for their involvement in corruption or serious human rights abuse.

"The United States is employing a new set of tools in Zimbabwe, including the flagship Global Magnitsky sanctions program, to make clear that the egregious behavior of some of the most powerful people and companies in Zimbabwe matches the actions of the worst human rights abusers and corrupt actors globally," said National Security Council Spokesperson Adrienne Watson announcing the action.

Concurrently, President Biden signed an Executive Order (E.O.) terminating the national emergency with respect to Zimbabwe and revoking the E.O.s that have authorized Zimbabwe-specific sanctions. As a result, the economic sanctions administered by OFAC pursuant to the Zimbabwe sanctions program are no longer in effect.

The President's E.O. of March 4, 2024, "Termination of Emergency With Respect to the Situation in Zimbabwe," terminated the national emergency

declared in E.O. 13288 and built upon in E.O. 13391 and E.O. 13469. As a result:

• All persons blocked solely pursuant to E.O. 13288, E.O. 13391, or E.O. 13469 (the authorities of the Zimbabwe Sanctions Program) will be removed today from OFAC's Specially Designated Nationals and Blocked Persons (SDN) List;

• All property and interests in property blocked solely pursuant to the Zimbabwe Sanctions Program will be unblocked today; and

• OFAC will remove the Zimbabwe Sanctions Regulations from the Code of Federal Regulations.

Sanctions Under The Global Magnitsky Program

➤ **Emmerson Mnangagwa (Mnangagwa)** is the President of Zimbabwe and is involved in corrupt activities, in particular those relating to gold and diamond smuggling networks. Mnangagwa provides a protective shield to smugglers to operate in Zimbabwe and has directed Zimbabwean officials to facilitate the sale of gold and diamonds in illicit markets, taking bribes in exchange for his services. Mnangagwa also oversees Zimbabwe's security services, which have violently repressed political opponents and civil society groups.

The First Lady of Zimbabwe, **Auxillia Mnangagwa**, has been included in the new designations. Both Mnangagwas have benefited from Zimbabwean businessman **Kudakwashe Regimond Tagwirei**, a close ally of Mnangagwa who has a longstanding association with the ruling party, the Zimbabwe African National Union-Patriotic Front (ZANU-PF). He has provided high-value gifts to senior members of the Government of Zimbabwe to gain access to resources and exerts significant control over major sectors of Zimbabwe's economy.

Included in the action are Zimbabwe's First Vice-President, Defense Minister and ruling party and security officials. [11877]

'Predator' Spyware Network Targeted

➤ OFAC designated two individuals and five entities associated with the **Intellexa Consortium** for their role in developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. government officials, journalists, and policy experts.

"Today's actions represent a tangible step forward in discouraging the misuse of commercial surveillance tools, which increasingly present a security risk to the United States and our citizens," said **Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson**.

Predator Spyware Sold To Customers Around The Globe

➤ Since its founding in 2019, the Intellexa Consortium has acted as a marketing label for a variety of offensive cyber companies that offer commercial spyware and surveillance tools to enable targeted and mass surveillance campaigns.

These tools are packaged as a suite of tools under the brand-name "Predator" spyware, which can infiltrate a range of electronic devices through zero-click attacks that require no user interaction for the spyware to infect the device. Once a device is infected by the Predator spyware, the spyware can be leveraged for a variety of information stealing and surveillance capabilities—this includes the unauthorized extraction of data, geolocation tracking, and access to a variety of applications and personal information on the compromised device.

The Intellexa Consortium, which has a global customer base, has enabled the proliferation of commercial spyware and surveillance technologies around the world, including to authoritarian regimes. Furthermore, the Predator spyware has been deployed by foreign actors in an effort to covertly surveil U.S. government officials, journalists, and policy experts. In the event of a successful Predator infection, the spyware's operators can access and retrieve sensitive information including contacts, call logs, and messaging information, microphone recordings, and media from the device.

Summit For Democracy

➤ In advance of the third Summit for Democracy, hosted by the Republic of Korea in Seoul on March 18, 2024. the designations align with steps announced in March 2023 around the second Summit for Democracy including the issuance of an Executive Order (E.O.) 14093 to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security; the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware; and the Guiding Principles on Government Use of Surveillance Technologies.

As described in E.O. 14093 and the White House Fact Sheet, commercial spyware has proliferated in recent years with few controls and a high risk of abuse.

The Intellexa Consortium

➤ **Tal Jonathan Dilian** is the founder of the Intellexa Consortium, and is the architect behind its spyware tools. The consortium is a complex international web of decentralized companies controlled either fully or partially by Dilian, including through **Sara Aleksandra Fayssal Hamou**. Ms. Hamou is a corporate off-shoring specialist who has provided managerial services to the Intellexa Consortium, including renting office space in Greece on behalf of **Intellexa S.A.**

Intellexa S.A. is a Greece-based software development company within the Intellexa Consortium and has exported its surveillance tools to authoritarian regimes. **Intellexa Limited** an Ireland-based company acts as a technology reseller and holds assets on behalf of the consortium. **Cytrox AD** is a North Macedonia-based company is a developer of the consortium's Predator spyware. **Cytrox Holdings ZRT** is a Hungary-based entity which previously developed the Predator spyware for the group before production moved to Cytrox AD in North Macedonia. **Thalestris Limited** is an Ireland-based that holds distribution rights to the Predator spyware and acts as a financial holding company for the Consortium. [11879]

ISTOCK

BIS

Freight Forwarder Guidance

The Bureau of Industry and Security (BIS) has issued guidance and best practices to enhance compliance among freight forwarders and exporters, collectively referred to as U.S. Principal Parties of Interest (USPPI). The guidance emphasizes the collaborative responsibility of freight forwarders and exporters in adhering to U.S. export controls and regulatory requirements.

Roles, Responsibilities, and Best Practices

Freight forwarders are defined under the EAR as entities authorized by a principal party to facilitate exports from the U.S., including arranging transportation. They must ensure compliance with EAR requirements based on information provided by service users, necessitating clear communication with the exporter/USPPI. Key responsibilities include:

- Securing detailed service expectations via Shipper's Letter of Instruction (SLI), Power of Attorney (POA), or equivalent authorizations.
- Adhering to the EAR's general prohibitions and being versed in export regulations from various federal agencies.
- Handling Electronic Export Information (EEI) filings in the Automated Export System (AES) accurately, whether on behalf of the exporter/

USPPI or providing assistance when the exporter/USPPI files their own EEI.

• Screening transactions against the Consolidated Screening List (CSL) and guiding exporters/USPPIs on compliance issues.

• Retaining records as mandated by EAR's Recordkeeping provisions.

The guidance further outlines best practices for freight forwarders, including rigorous screening for restricted parties, collaborating with exporters/USPPIs on compliance matters, and engaging in continuous education on industry standards and regulations.

Export Transactions: Non-Routed and Routed

For non-routed export transactions, the exporter/USPPI bears primary responsibility for EEI filing, either directly or through a U.S. authorized agent. In routed transactions, the Foreign Principal Party in Interest (FPPI) oversees export facilitation and EEI filing, necessitating authorization for a U.S. agent to act on their behalf.

Antiboycott Compliance

The document highlights the importance of adhering to U.S. antiboycott regulations, which prohibit participation in unsanctioned foreign boycotts. U.S. persons, including freight forwarders, are required to report receipt of boycott requests and are advised against engaging in activities that support such boycotts.

Red Flags for Forwarders:

• ECCN/EAR99 and license authorization type (license number, license exception, no license required) not provided by the exporter/USPPI when requested.

• The exporter/USPPI does not provide a Power of Attorney (POA) or other written authorization to file the EEI.

• Exporter/USPPI routinely omits required EEI data elements.

• Exporter/USPPI is unfamiliar/unable to answer questions regarding applicability of the EAR or other export regulations to their export shipments.

• Exporter/USPPI is unfamiliar with/unable to answer question regarding its customers or the destination of the items being exported.

• Routed transactions are paid for and/or arranged by a company in a country different than the destination of the export and with no apparent connection to the transaction (e.g., not a parent/sibling/subsidiary company).

• Party listed as the ultimate consignee does not typically engage in business consistent with consuming or otherwise using subject commodities.

• A party's address is similar to that of a party on a proscribed party or sanctions list, or their physical location is unusual (e.g., business address is a residence).

• The exporter/USPPI or an FPPI in a routed transaction requests a document certifying the carrying vessel is not blacklisted or is allowed to enter a named Arab country port.

• The freight forwarder is requested to certify no parties involved in the transaction, including the shipping line agent, are of Israeli origin.

• Forwarder (authorized agent) filed an EEI and does not provide the USPPI with an EEI filing report upon request.

• Forwarder does not require a POA or other written authorization from USPPI for a routed export.

• ECCN/EAR99 and license type (license number, license exception, no license required) not requested when a forwarder is filing an EEI or when an exemption legend is being used in lieu of an EEI filing.

• The forwarder is not supportive or communicative regarding the services they are providing.

• AES filings made by forwarder on behalf of the exporter/USPPI routinely contain inaccurate information.

• Forwarder unable to recognize license exceptions codes provided by the exporter.

• Forwarder unfamiliar with the EAR or other export regulations.

• Forwarder (authorized agent) does not obtain a POA or other written authorization prior to filing an EEI.

• AES response messages are not being addressed, as appropriate.

• Forwarder routinely uses exporter/USPPI information for AES filings the exporter/USPPI did not authorize.

• Forwarder requests certification that no parties or commodities involved in the transaction are of Israeli origin.

A link to the full guidance can be found in the full story [11973]

To read complete articles, click on the Story ID number.