

The Export PractitionerTM

SEPTEMBER
2022

VOLUME 36
NUMBER 9

Timely News and Analysis of Export Regulations

INSIDE

**"New Space" and the
MTCR**

**Arms Trade Treaty
Conference: Focus on
Diversion**

**Are Sanctions on
Russia Working?**

**"Hoskins" an FCPA
must read**

**State Debars Cyber
Job Hoppers**

Latin Corruption

**AI Chip Restrictions
Get Real**

**New Controls on
Semiconductor Tools
and Gas Turbines**

**BIS publishes "Red
Flags" list for Russia
Sanctions**

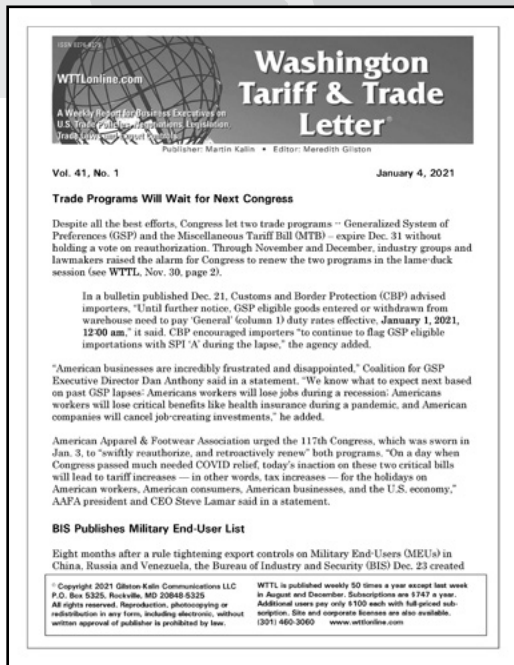
**Aerospace Sanctions
Expand**

**OFAC Rewrites Cyber
Sanctions**

And More...

Get the Trade News you need
EVERY WEEK with...

WASHINGTON TARIFF & TRADE LETTER



With WTTL, you will stay ahead of developments at:

The U.S. Trade Representative's Office
Bureau of Industry & Security
International Trade Administration
International Trade Commission
Treasury's Office of Foreign Assets Control
Court of International Trade
State's Directorate of Defense Trade Controls
Export - Import Bank
Congress
Customs and Border Protection
and more...

Keep Posted on Trade Disputes and Export Opportunities in:

China | Japan | European Union | Middle East
Africa | Brazil | Central America | Mexico
Korea | Caribbean | India | Vietnam | Canada
Argentina | Colombia | Pakistan | Thailand
Morocco | Turkey | Australia

Your interest in Washington trade policy goes far beyond U.S. export controls and trade sanctions. You need to follow policy decisions, trade disputes and legislation.

You need to know what is happening on:

- Section 232 Tariffs
- Antidumping and Countervailing Duty Cases
- WTO Trade Negotiations
- Trade Sanctions on Iran, North Korea, Cuba
- Bilateral Trade Disputes
- Trade Legislation
- Customs Requirements
- Court Decisions on Trade
- Antiboycott Enforcement
- Foreign Corrupt Practices Act Cases
- Trade Promotion
- China Market Access
- NAFTA

*Every week, 50 issues a year,
Washington Tariff & Trade Letter
delivers advance, exclusive reports that provide
the full spectrum of news on trade issues of
concern to you.*

For more information on **Special Discount** and
Free Sample, Call Frank at 301-460-3060

www.WTTLOnline.com

The Export Practitioner

SEPTEMBER 2022
Volume 36
Number 9

Publisher

Martin Kalin

Editor

Frank Ruffing
+1.703.283.5220
fruffing@traderegs.com

The Export Practitioner
Is published monthly by
Gilston-Kalin Communications, LLC
P.O. Box 5325,
Rockville, MD 20848-5325

www.exportprac.com

On the cover:

Long exposure of the SpaceX
Crew-2 launch April 23, 2021 from
Kennedy Space Center, viewed over
the Indian River. (Daniel Hull)

AT A GLANCE

4 | FEATURE

“New Space” and the Missile Technology Control Regime
“State of Space” Report on Industrial Base

DEPARTMENTS

7 | POLICY BRIEFS

- UN Report on Uyghur “Crimes Against Humanity”
- Arms Trade Treaty Conference: Focus on Diversion
- Are Sanctions on Russia Working?
- ITA Calls for Comments on AI Competitiveness
- USTR Notorious Markets List

10 | FOCUS ON ENFORCEMENT

- “Hoskins” an FCPA must read
- State Debars Cyber Job Hoppers
- TDO on Belgian Trader
- Romanian Petro Fraud
- Odebrecht Stench Still Wafts
- Petropiar Bribery and Money Laundering
- Paraguayan Leaders Deemed Corrupt
- Justice returns Nigerian Funds, Stolen by Former President
- Low-Level Crypto Washer Extradited to U.S.

13 | EXPORT CONTROLS

- China Blacklist Grows
- AI Chip Restrictions Get Real
- New Controls on Semiconductor Tools and Gas Turbines
- Iran General License M-2 Education Services
- YMTC Shoe to Drop?
- US Defense Contractor Plans “ITAR Free” Drone Subs

15 | TRADE SANCTIONS

- BIS publishes “Red Flags” list for Russia Sanctions
- Aviation Sanctions Expand
- OFAC Rewrites Cyber Sanctions
- Landmark Crypto Sanction
- UK Sanctions Reporting Guide

“New Space” and the Missile Technology Control Regime

Commercial space activities have risen over the last few decades, changing dynamics in the global industry. New actors, states and companies, have emerged and participation in the space industry is slated to only continue expanding.

Manufacturing in particular is at the center of this rise in activities. Coupled with the inherently dual use nature of space technologies, the result has been increasing access to space launch vehicles and related technologies. This raises questions concerning potential missile proliferation risks and threats these may pose to the Missile Technology Control Regime (MTCR).

Since 1987 the MTCR has aimed to limit the spread of ballistic missiles and other unmanned delivery systems that could be used for chemical, biological, and nuclear attacks. The MTCR is the multilateral export control regime through which participating supplier states coordinate their export control policies and share information. Signatories agree to restrict their exports of missiles and related technologies capable of carrying a 500-kilogram payload at least 300 kilometers or delivering any type of weapon of mass destruction.

The Stockholm International Peace Research Institute (SIPRI) hosted a panel August 16th to discuss this challenge, with **Almudena Azcárate Ortega** of the Space Security and WMD Programmes, United Nations Institute for Disarmament Research, **Andrew Horton**, Chair, Technical Experts Meeting, MTCR and Government Senior Advisor on Export Control Technical Policy, British Government, and **Alan Thompson**, Head of Government Relations, Skyrora Ltd, the Scottish launch systems builder. The discussion was moderated by **Nivedita Raju**, Researcher, Weapons of Mass Destruction (WMD) Programme, SIPRI. Extracts of the conversation follow. A recording of the entire program is available [here](#).

Almudena Azcárate Ortega: Let's talk about the definition of new space I don't really think there is a one-size-fits-all definition. The concept of new space is generally used to refer to commercial space companies that have emerged in recent years, and although each company is of course different, they might have their own objectives and interests: some focus on small satellites, mega constellations others do launch servicing and others do on orbit servicing, or even space tourism. So even though

they might be very different they do seem to share a goal, and this is a goal of wanting to make space more accessible.

They tend to be adaptable; they tend to be willing to adopt new technologies, and they tend to favor structures that are similar to those that we know from Internet startups. For example,

they often have a global outlook that that means that they don't really seek to become contractors of just one state or a specific space agency like the old school space companies in the 60s when the race to the moon was going on. Rather they market themselves to international customers and even sometimes to private individuals. The term New Space is also used to refer to not just these companies themselves, but also to the shift that the

commercial space industry has seen in these recent years from those big traditional companies that I was referring to.

I think it's around an 80% of space activities that are carried out by commercial companies, but also these new space companies have made space more accessible worldwide. New Space companies seem to be known for their ingenuity, their willingness to develop new technologies and all of these characteristics seem very positive. However, they do raise certain concerns from a security perspective.

This increase accessibility can mean increase dangerous proliferation of technologies that could be weaponized. I've talked about ADR which is active debris removal, on orbit servicing, and the similarity between space launch vehicles and ballistic missiles. This is not new. Missile technology has been repurposed to serve as space launch vehicles since the very first experimentations to go into space. The V2 rocket, which was used as the basis by the Soviet Union to develop their first ICBM, was modified to launch Sputnik 1. It also evolved into the US Saturn V rockets which would eventually take humankind to the moon.

This link can still be seen today. For example, the U.S. Minotaur family of space launchers use stages of the MX peacekeeper ICBM. It also has worked the other way round. States could use or develop ballistic missile technology or ballistic missile components from technology that they have acquired from space launch programs.

Though there are differences between space launch vehicles

New Space companies seem to be known for their ingenuity, their willingness to develop new technologies and all of these characteristics seem very positive. However, they do raise certain concerns from a security perspective.

and ballistic missiles, they do have certain similarities that we have to be aware of, and that rightfully raise concerns among States and among other stakeholders. It's important to be aware and be compliant with control regulations in order to be able to mitigate this threat of proliferation.

Andrew Horton: I want to touch on some of the aspects less about the technology side, because I think it's fairly well known the similarities between space launch vehicle technology and ballistic missile technology. There's a key point here when it comes to New Space, where we're looking at smaller launchers, which are probably closer to ballistic missiles in terms of their underlying technology and the capability that they have.

What's of greater challenge to the export control community is the range of new actors that are involved in this, rather than the actual underlying technology. The MTCR over the years has developed quite an extensive list, called the "key technologies" that are used in sort of ballistic missiles and so forth, but I think what's new for the regimes, I say regimes here because there's also the Wassenaar Arrangement, a key export control which covers much of the same technology, are the actors.

We have a range of new actors, both state and non-state, involved with this who have access to technology but have less experience, who don't quite have the culture of export controls and complying with regulations. The sort of historic aerospace defense companies that were traditionally involved in space, they were very much linked to the states. They understood regulatory requirements particularly around export controls. Now we're having a new set of entrepreneurial actors in this space that don't necessarily appreciate or understand the sensitivities of the technology and the need to control them with export controls.

We also have new actors on the government side, "space regulators," the sort of people that are there to promote investment and development. In this again they're doing their job, but they don't necessarily have a fuller understanding of the sensitivities of the technology and the requirement around protecting those technologies. In addition, there's a new ecosystem in terms of the market and how these sorts of companies are looking to promote their services on a global level. So again, there are new challenges that we haven't seen before.

Within the MTCR there's a need to understand both the actors and the ecosystem that's out there, and potentially to move away from focusing so much on traditional export controls and more towards how we can build a better sort of confidence in the emerging space sector, so they're looking more towards the sort of transparency and confidence building measures to provide a

What's of greater challenge to the export control community is the range of new actors that are involved in this, rather than the actual underlying technology.

code of conduct for example. To move away from traditional export controls as being the sole reliance mechanism for controlling the proliferation of technology, but moving towards something that's a little bit more sort of collegial in terms of transparency and confidence. But the question is, how do you achieve that without letting the genie out of the bottle in terms of the sort of full proliferation of ballistic missile technologies?

Alan Thompson: I think one of the huge other things that is perhaps somewhat overlooked is that, as far as I'm concerned, it's very much focused on the physical control of items and elements rather than the control of data. I know it does affect data, but

I think the other elephant in the room is the element of cyber security and the transfer of data. How does this work in this context? Indeed when I first started talking with colleagues on this topic the challenge is it's not so much about the physical controls, because usually by the time you get to a physical control it's already too late.

I think that traditionally the commercial space sector has not been too engaged with the space security community and they wanted to remain removed from it, due to wanting to be removed from the idea of contributing potentially to conflict in space, that sort of thing. What the new space dynamic represents to the missile technology control regime is, from our point of view we really want to engage. We want to demonstrate that we are responsible not just on the technical side of things, not just with the missile technology control regime, but also with the other aspirations which go above that, with peace and environmental challenges that we're being faced with. I think that that's an aspiration I am voicing on behalf of the space industry. I do think that we want to do this responsibly and this is the reason why we're desperately keen to be involved in these discussions.

Andrew Horton: Traditionally export control regimes have always been very focused on those physical widgets and bits of kit and components and has been less focused on the technology. Of particular concern is the transfer of technology, and how it can now be done intangibly through pressing the return button on your laptop on that file shoots off. That's often the sort of challenge that we have within the export control regimes.

We have for a number of years been talking to partners around the capability with satellites, for example earth observation satellites are a key sort of element within the use of strategic systems, certainly in terms of providing targeting information - targeting data for ballistic missiles, providing navigation and guidance for cruise missiles. So it's not simply about the missile technology being transferred it's about the transfer of strategic capabilities through access to commercial space itself.

Almudena Azcárate Ortega there is actually interest from the state's perspective to encourage the engagement of commercial actors to engage directly with them because, as you as you might know, under the outer space treaties states are responsible for the activities of their nationals. This includes non-governmental entities such as the commercial space industry so it is in a state's interest to ensure that the commercial space industry is knowledgeable of the regulations and that they comply with them, so that the state itself is not responsible at the international level if something goes wrong.

Alan Thompson: There are huge amounts of regulations out there that we don't even know, so we start from a point of ignorance. We don't know where to go to even start understanding if this is regulated or not, partly because a lot of these regulations occurred when the government put them in place for their service providers who made these ballistic missiles all those years ago. This is easily accessible in our countries, but this can be a bit more tricky for countries that are starting out. They might not have that infrastructure.

I think there's an important piece of work that needs to be done by international bodies. For example the MTCR needs to pick up its game in this area, but I would also point to organizations like the International Civil Aviation Authority. Regulators need to promote awareness. One of the challenges is that we don't have a space launch or space operation equivalent to the International Atomic Energy agency so there isn't that single international global body that you can go to for that information.

I think I would prefer to see the export controls and the MTCR more as an enabler rather than a limiter because that's exactly what it was there for in the first place. The MTCR was a regime and agreement between countries that this is how they wanted to regulate this collaboration. I think the perception is at the moment that MTCR is actually a limiter. The perception is that ITAR is a limiter. It's not. It's a way that governments have agreed to be able to allow things to happen, to enable things. I think it's only for the nefarious actors that control regimes are a problem.

State of the Space Industrial Base Report

"While the United States space industrial base remains on an upward trajectory, the upward trajectory of the People's Republic of China is even steeper, with a significant rate of overtake, requiring urgent action."

So concludes the "[The State of the Space Industrial Base 2022 Workshop Report](#)" the annual interagency and industry review sponsored by the Space Force, Defense Innovation Unit, and Air Force Research Laboratory.

"Specifically, the U.S. lacks a clear and cohesive long-term vision, a grand strategy for space that sustains economic, technological, environmental, social and military (defense) leadership for the next half century and beyond," the report asserts, noting limited progress on the recommendations of [last year's report](#).

Included in the report's 110 pages are illustrations of the state of play and working group suggestions, including a call for "review of ITAR lists, and the removal of technologies available in the international marketplace," and the treatment of space as a "Priority Export Activity."

The recommendation is that lists of restricted exports be reviewed and updated on a one-to-three-year cadence to ensure the technology still requires controls. "If a company believes their technology is dual use, or commercially available, a two-page white paper should be adequate to force an expedient export review."

The calls for greater subsidies range from the opaque: "non-dilutive capital, procurement, advance-market commitments, and debt instruments the USG can provide and align them to the taxonomy of challenges," to the ludicrous: "designate Space as an economic opportunity zone in order to improve the economic prospects for critical space-technologies or infrastructure," and "a Homestead Act for Space."

No word yet of an astral expansion of the General Mining Law of 1872 or the Pacific Railroad Acts of 1862.

There are huge amounts of regulations out there that we don't even know, so we start from a point of ignorance.



UN Releases Long-Delayed Report on Uyghur “Crimes Against Humanity”

Minutes before midnight on her last day as U.N. High Commissioner for Human Rights, Michelle Bachelet authorized the release of a harshly critical [report](#) of China’s treatment of Uyghurs and other predominantly Muslim communities, detailing in all but name the genocidal treatment of the Turkic minority.

“Allegations of patterns of torture, or ill-treatment, including forced medical treatment and adverse conditions of detention, are credible, as are allegations of individual incidents of sexual and gender-based violence,” said the report.

The extent of arbitrary detentions against Uyghur and others, in context of “restrictions and deprivation more generally of fundamental rights, enjoyed individually and collectively, may constitute international crimes, in particular crimes against humanity.”

China’s attached rebuttal, thrice the length of the report, contends the Vocational Educational and Training Centers (VETCs), or re-education camps are “learning facilities established in accordance with law intended for de-radicalization” and not “concentration camps”.

A spokeswoman for U.N. Secretary General Antonio Guterres said Mr. Guterres “values the system-wide cooperation between China and the United Nations on a whole host of issues. China is a very valuable partner, and we very much hope that that cooperation will continue,” and urged it was “important for everyone to see the Chinese response” to the detailed report.

The Xinjiang Uyghur Autonomous Region produces about one-fifth the world’s cotton, half the world’s polysilicon, and is home to the world’s second largest manufacturer of polyvinyl chloride (PVC).

The Uyghur Forced Labor Prevention Act (UFLPA), effective June 21, places few restrictions on the import of those commodities when reprocessed in third countries.

Arms Trade Treaty Conference: Focus on Diversion

Post-shipment on-site inspections are one of the main focuses of the German presidency of the Eighth Conference of States Parties (CSP8) to the 2013 Arms Trade Treaty (ATT), which took place on 22–26 August in Geneva. The ATT is the first legally binding international agreement that aims to establish common standards for regulating the trade in conventional arms.

In advance of the conference, the Stockholm International Peace Research Institute (SIPRI) published two papers on post shipment inspections and stockpile management systems which help to inform manufacturers and exporters of the military materiel that will be the focus of controls on the value of on-site inspections and the opportunities to integrate the topic in design.

The ATT is the first legally binding international agreement that aims to establish common standards for regulating the trade in conventional arms.

States that adopt post-shipment on-site inspections shall continue to fully apply the export licensing assessment criteria that they are legally or politically required to implement, such as those under the ATT, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (Wassenaar Arrangement), and the European Union (EU) common position on arms exports.

A growing number of states and international and regional organizations, provide assistance for the management and accountability of states’ small arms and light weapons (SALW) stockpiles. This support is generally categorized as

physical security and stockpile management (PSSM) assistance.

On-site inspections are a focused, short-term verification measure mainly aimed at ensuring that exported weapons have not been transferred in ways that contravene commitments provided by the importer. PSSM assistance is a longer-term engagement aimed at improving a state's system of weapons management over time.

The authors note that on-site inspections cannot replace the need for accountability throughout the life cycle of a weapon, which begins with effective and verifiable record-keeping. For example, in Afghanistan, end-use monitoring officials of the USA-led Combined Security Transition Command-Afghanistan (CSTC-A) used a centralized, worldwide US Government system, the Security Cooperation Information Portal (SCIP), to record weapons distributed to Afghan security forces and subsequent end-use checks. However, CSTC-A colleagues simultaneously rolled out a separate database, CoreIMS, to Afghan security forces to register and manage these weapons themselves. This led to dilution of registration and data entry efforts in both systems. Only about 40 per cent of items distributed by the US Government were ever actually recorded in the SCIP, according to a 2019–20 audit.

The US Army, among others, has used radio frequency identification devices embedded in ammunition packaging, and even in individual weapon systems

The US Army, among others, has since 2005 used radio frequency identification (RFID) devices embedded in ammunition packaging, and even in individual weapon systems in some cases, to automatically record when items enter and leave armories and magazines, and when they arrive in or depart from the possession of different units. Conflict Armament Research and TTE-Europe GmbH, funded by the EU, have begun trialing RFID devices suitable for placement in individual small arms themselves.

SIPRI recommends that states conducting on-site inspections should explore requiring either manufacturers or importers to adopt and use RFID chips or other detectable tracking technologies, both as a means of inspection visits and as a means through which the importing state can improve its PSSM standards.

Are Sanctions on Russia Working?

The debate continues on the utility and efficacy of US-led economic sanctions in isolating and weakening Russia.

A new study by the Yale School of Management has published data that supports the US government's view that the sanctions imposed on Russia have jeopardized its economy. According to the study, more than 1,000 international firms have left Russia in the wake of the Ukraine war.

"As a result of the business retreat, Russia has lost companies representing ~40% of its GDP, reversing nearly all of three decades' worth of foreign investment and buttressing unprecedented simultaneous capital and population flight in a mass exodus of Russia's economic base."

In particular, the sanctions have devastated Russia's foreign technology-dependent automotive, aviation, and arms industries. At the same time, Russian gross domestic value-added indicators have fallen by 62 percent in the construction sector, 55 percent in agriculture, and 25 percent in manufacturing.

Russia expects to enjoy a current account surplus of \$265 billion this year, thanks to robust commodity exports. The IMF projects Russia's GDP to shrink by 6% in 2022, far from a "knockout blow."

According to the IEA, Russia's exports of crude and oil products to Europe, the US, Japan, and Korea have fallen by nearly 2.2 mb/d since the start of the war, but the rerouting of flows to India, China, Turkey and others, along with seasonally higher Russian domestic demand has mitigated upstream losses. By July, Russian oil production was only 310 kb/d below pre-war levels while total oil exports were down just 580 kb/d.

The EU embargo on Russian crude and product imports that comes into full effect in February 2023 is expected to result in further declines, as some 1 mb/d of products and 1.3 mb/d of crude would have to find new homes. Prices realized by the Kremlin are lower as well. The Yale report [notes](#) the spread between Brent and Ural (Russian) benchmarks has widened to \$35 per barrel, reflecting discounts extracted by Asian buyers.

While the sanctions have cut Russian access to Western financial institutions, Russian firms continue trade through countries like the United Arab Emirates and Turkey which have chosen not to join the allied sanctions. [Reuters reports](#) that Turkey is being used as a "warehouse and bridge" by European businesses to supply goods to Russia.

The Royal United Services Institute, the British defense and security think tank [reports](#) that more than 450 foreign-

made components have been found in Russian weapons recovered in Ukraine, suggesting critical technology was acquired by Russia from Western countries years before the invasion. According to the research, when disassembled, 27 Russian weapons and military systems were found to rely predominantly on Western parts, with almost two-thirds of the components manufactured by US-based companies.

ITA Calls for Comments on AI Competitiveness

The Commerce Department's International Trade Administration (ITA) is requesting public comments to gain insight on the current global AI market and stakeholder concerns regarding international AI policies, regulations, and other measures which may impact U.S. exports of AI technologies. ITA seeks broad input from all interested stakeholders—including U.S. industry, researchers, academia, and civil society—on the potential opportunities for and challenges to increasing U.S. export competitiveness for AI-enabled technologies.

The initiative, led by Barton Meroney, Executive Director, Office of Manufacturing Industries, seeks to answer 12 questions, ranging from ranging from standards and IP protection to how AI can be incorporated in future trade agreements. Comments to be submitted in writing by October 17, 2022

Notorious Markets List (Special 301 Review)

USTR requests comments that identify online and physical markets to be considered for inclusion in the 2022 Review of Notorious Markets for Counterfeiting and Piracy (Notorious Markets List).

The Notorious Markets List identifies examples of online and physical markets that reportedly engage in or facilitate substantial copyright piracy or trademark counterfeiting. The issue focus for the 2022 Notorious Markets List will examine the impact of online piracy on U.S. workers. Announcement [[87 FR 52609](#)]

Is a Site or Corporate License for You?

- When many individuals in your organization need to read ***The Export Practitioner*** every month, there's an easy way to make sure they get the export compliance information they must have quickly and conveniently.
- That's through a site or corporate license giving an unlimited number of your colleagues access to a print or online version of ***The Export Practitioner***.
- With a low-cost site or corporate license, you can avoid potential copyright violations and get the vital information in each issue of ***The Export Practitioner*** to everyone who should be reading it.
- **For More Information and Pricing Details, Call: 301-460-3060**

Hoskins an FCPA must read.

In finding inculpable a foreign employee for his involvement in a bribery scheme, the US Court of Appeals for the Second Circuit offers a slender reed for an FCPA defense campaign.

The appeals court held August 12th that “the district court properly granted Hoskins’s motion for judgment of acquittal for violations of the FCPA because there was no agency or employee relationship between Hoskins and Alstom Power, Inc. We also affirm the district court’s Speedy Trial Act and Sixth Amendment rulings, as well as its instructions to the jury about withdrawal from a conspiracy and venue in the District of Connecticut.”

The American subsidiary of Alstom Power, Inc. (“API”), a global power and transportation services company, hired two consultants to bribe Indonesian officials to help secure a \$118 million power contract. Lawrence Hoskins, who worked in Paris for API’s United Kingdom subsidiary, was allegedly responsible for approving the selection of the consultants and authorizing payments to them.

For his role in the alleged bribery scheme, Hoskins was charged in an American court with (among other things) violating the Foreign Corrupt Practices Act (“FCPA”), which makes it unlawful for officers, directors, and agents “of a domestic concern” to use interstate commerce corruptly to bribe or attempt to bribe foreign officials. 15 U.S.C. § 78dd et seq.

Because Hoskins is not an American citizen, was not employed by the American subsidiary, and did not enter the United States while allegedly working on the scheme, he falls outside the category of persons directly covered by the FCPA. The government nevertheless contended that Hoskins was liable under the FCPA as a co-conspirator or accomplice to the American subsidiary’s FCPA violation.

United States v. Hoskins, US Court of Appeals for the Second Circuit, August 12, 2022

State Debars Cyber Job Hoppers

Three Cybersecurity contractors were debarred for ITAR violations after their U.S. employer lost a contract with the UAE government and they continued their work for the foreign incumbent.

The services performed constituted furnishing defense services under U.S. Munitions List (USML) Category XI(d) because: (a) the relevant systems were electronic systems, equipment, or software that were specially designed for intelligence purposes that collect, survey, monitor, exploit, analyze, or produce information from the electromagnetic spectrum as described in USML Category XI(b); and (b) Assisting foreign persons in the use, design, development, en-

gineering, production, modification, testing, maintenance, processing, or operation of the relevant systems.

Respondents did not have a license or other approval to furnish such ITAR-controlled defense services.

TDO on Belgian Trader for China Aerospace Tech Sales

The Commerce Department imposed a temporary denial order of export privileges of Hans De Geetere of Belgium and his company Knokke-Heist Support Corporation Management, also known as Hasa-Invest to prevent an imminent violation of Export Administration Regulations.

According to the Order, De Geetere and his company repeatedly acquired or attempted to acquire under false pretenses accelerometers from the United States on behalf of prohibited end-users or for prohibited end-uses in China.

The use of accelerometers by the aerospace and defense industries, and Respondents’ false statements made to U.S. companies to obtain the items, raises significant concerns of future violations absent the issuance of a TDO.

Among the violations, OEE cited a letter in support of an end-user statement that was purportedly signed by the Belgian Government. In an attempt to get a shipment released, U.S. authorities were provided a BIS Form 711 dated April 15, 2021, and signed by “De Geetere H,” identified as the CEO of Knokke-Heist, asserting that the end-user was a Belgian Government agency.

OEE was unable to confirm the alleged Belgian Government end-user, at which point a fraudulent e-mail was sent to OEE, purporting to be from the Belgian Government, supporting the end user document.

Prior to the April 2021 detained shipment, De Geetere had been ordering U.S. origin accelerometers via a German Distributor, coincident with the U.S. firm’s Chinese distributor, Shanghai Nova Instruments Company, Ltd, being placed on the Entity List for being “involved in the procurement of items subject to the EAR for possible use in missile and unmanned aerial vehicle applications in China without the licenses required pursuant to §§ 744.3 and 744.21 of the EAR.”

OEE asserts that at least some of Respondents’ orders were placed on behalf of China Aerospace Research Institute, an entity BIS has reason to believe is connected to or is an alias for the China Aerospace Science and Technology Corporation (“CASC”) 1st Academy 12 Research Institute, a party also on BIS’ Entity List.

OEE later became aware of two June 2021 shipments of accelerometers by U.S. Company 1 to a recently incorporated United Arab Emirates-based company (“UAE Company 1”). Given the size of the second shipment and UAE Company 1’s recent incorporation, the second shipment was detained to verify its bona fides and conduct a post-shipment

verification (“PSV”) of the first and smaller shipment of accelerometers to UAE Company 1. Among other things, the PSV determined UAE Company 1 did not possess the type of equipment that could utilize the accelerometers at issue and did not make available either the items or records confirming their ultimate destination.

Additionally, the PSV found that a fictitious name was used by the UAE Company when dealing with the U.S. Manufacturer.

Further investigation revealed that the UAE Company purchased the items on behalf of Knokke-Heist and had forwarded the first shipment to Respondents using an address in the Netherlands. Moreover, other evidence gathered indicates that De Geetere was assisting the UAE Company in responding to the detention and subsequent seizure of the second shipment by the U.S. Government.

The investigation also uncovered facts that indicate that De Geetere led the UAE Company to believe that the items were for ultimate use by a Belgian Government entity; the same fraudulent scheme De Geetere and Knokke-Heist employed directly with the U.S. Manufacturer several months earlier.

Additional attempts by Knokke-Heist to acquire the same model of accelerometers were made to several other European distributors of the U.S. manufacturer, along with a separate attempt to acquire the items directly from a U.S. company located in Florida. Most recently, Belgian authorities identified a mid-August 2022 shipment of accelerometers from the United States to Knokke-Heist.

Given the sheer number and nature of attempts by De Geetere and Knokke-Heist to acquire U.S.- origin items under false pretenses on behalf of prohibited end-users or for prohibited end-uses, OEE deems a TDO necessary to prevent future violations.

Justice Returns Funds from Romanian Petro Fraud

The Department of Justice announced today that more than \$1.2 million in forfeited funds from an international tax fraud and money laundering case will be returned to the government of Romania. The funds are the proceeds of the sale of property located in the State of Washington that were owned by a Romanian couple who were extradited back to Romania at the request of the Romanian government.

According to records filed in the U.S. District Court for the Western District of Washington, in 2012, Romanian authorities asked the United States to extradite Radu and Diana Nemes to Romania to face charges of tax evasion and participating in an organized criminal group. The charges alleged that the Nemeses executed a scheme to avoid Romanian taxes on imported diesel fuel by claiming the fuel was a

lower grade of industrial and maritime fuel. The untaxed income from the sale of the higher value diesel was laundered through a number of bank accounts and shell companies controlled by the Nemeses.

Arrest warrants for the couple were issued in Romania in July 2012. Sometime before those warrants, the Nemeses had left Romania and resided near Yelm, Washington, on a large piece of property with an elaborate bunker system. Following their arrest in the United States, the couple waived extradition and agreed to be returned to Romania in early 2014.

The couple’s assets in the United States were forfeited, including Yelm properties which were sold as part of the forfeiture process. The proceeds of that sale, \$1,225,465, are being returned through a petition for remission to the government of Romania as a recovery on the tax fraud. The overall tax fraud scheme resulted in a \$58.677 million loss to the Romanian government.

Odebrecht Stench Still Wafts

The Department of Justice is returning approximately \$686,000 in forfeited criminal proceeds to the Republic of Peru linked to the corruption and bribery of former Peruvian President Alejandro Celestino Toledo Manrique (Toledo) by Odebrecht S.A. (Odebrecht), the Brazil-based global construction conglomerate.

Justice alleged that Toledo, who was the president of Peru from approximately 2001 to 2006, solicited millions in bribery payments from Odebrecht while he was in public office in connection with government contracts awarded for construction of the Peru-Brazil Southern Interoceanic Highway (Southern Interoceanic Highway), a Peruvian government infrastructure project. Odebrecht subsequently made bribery payments to Toledo through accounts maintained by Toledo’s co-conspirators.

Ultimately, approximately \$1.2 million of the bribery payments were used by Toledo and his family to purchase real estate in Maryland in 2007 through a scheme designed to hide Toledo’s ownership of the funds and their connection to Odebrecht. The forfeited assets represent the proceeds from the sale of the Maryland real estate, which were further laundered through a trust and bank account controlled by Toledo.

Venezuelan Charged in \$30M Petropiar Bribery and Money Laundering

A federal grand jury in Miami returned an indictment August 24 charging a Venezuelan national for laundering

the proceeds of substantially inflated procurement contracts obtained by making bribe payments to senior officials at Petropiar S.A.

Petropiar is a joint venture between PVDSA and Chevron engaged in hydrocarbon exploration, drilling, transport and storage in the Orinoco oil belt, Venezuela.

According to the indictment, from at least 2015 through at least May 2019, Rixon Rafael Moreno Oropeza, 46, allegedly engaged in a scheme to obtain multimillion-dollar contracts from Petropiar by paying bribes to senior officials at Petropiar. Moreno allegedly agreed to pay a \$1 million bribe to a senior official in the Venezuelan government to install another person as a high-ranking official in the procurement division of Petropiar. In addition, Moreno allegedly sent millions of dollars in bribe payments to senior Petropiar officials from accounts he controlled in South Florida. In exchange for these bribe payments, Moreno allegedly received benefits including over \$30 million in payments on contracts from Petropiar to accounts Moreno controlled in South Florida.

Illustrative of this, Moreno received approximately \$2.7 million from a Petropiar contract to supply breathing devices, a contract whose price had been allegedly inflated to 100 times the actual cost. Moreno allegedly used the proceeds obtained from the Petropiar contracts for his own personal benefit, including to purchase real estate, a private jet, and luxury vehicles in South Florida.

Paraguayan Leaders Deemed Corrupt.

The State Department is designating Paraguayan Vice President Hugo Velazquez and Yacyretá Bi-National Entity Legal Counsel Juan Carlos “Charly” Duarte for involvement in significant corruption, including bribery of a public official and interference in public processes. Velazquez has announced his resignation.

The allegations come several weeks after Paraguay’s former president Horacio Manuel Cartes was included in a US corruption list for involvement in “significant corruption.”

Electricity generation in Paraguay is dominated by the large binational hydropower projects of Itaipu (Brazil-Paraguay) and Yacyretá (Argentina-Paraguay) which provide over 99% of the country’s electricity and generate a large electricity surplus for export

“Historically, officials in all branches and at all levels of government have engaged in corrupt practices. Judicial insecurity and corruption mar Paraguay’s investment climate,” according to State’s [Investment Climate Statements](#).

Justice returns \$23M Nigerian Funds, Stolen by Former President.

The United States, through the Department of Justice and FBI, forfeited approximately \$23 million traceable to the corruption and money laundering of former Nigerian dictator Sani Abacha and his co-conspirators. This money will be returned to the Nigerian people through an agreement between the Governments of the United States and the Federal Republic of Nigeria. This repatriation will bring the total amount forfeited and returned by the Department of Justice in this case to approximately \$334.7 million.

In 2014, U.S. District Judge John D. Bates for the District of Columbia entered a judgment ordering the forfeiture of approximately \$500 million located in accounts around the world, as the result of a civil forfeiture complaint for more than \$625 million traceable to money laundering involving the proceeds of Abacha’s corruption. In 2020, the department repatriated over \$311.7 million of the forfeited assets that had been located in the Bailiwick of Jersey. Last year, the U.K. government enforced the U.S. judgment against the additional \$23 million.

Low-Level Crypto Washer Extradited to U.S.

An alleged cryptocurrency money launderer was extradited from the Netherlands to the United States to face Federal charges. Denis Mihaqlovic Dubnikov, 29, a Russian citizen, made his initial appearance in federal court August 17 in Portland, Oregon.

According to court documents, Dubnikov and his co-conspirators laundered the proceeds of ransomware attacks on individuals and organizations throughout the United States and abroad. Specifically, Dubnikov and his accomplices laundered ransom payments extracted from victims of Ryuk ransomware attacks.

In July 2019, Dubnikov allegedly laundered more than \$400,000 in Ryuk ransom proceeds. Those involved in the conspiracy laundered at least \$70 million in ransom proceeds. First identified in August 2018, Ryuk is a type of ransomware software that, when executed on a computer or network, encrypts files and attempts to delete any system backups. In October 2020, law enforcement officials specifically identified Ryuk as an imminent and increasing cybercrime threat to hospitals and healthcare providers in the United States.

China Blacklist Grows

The Commerce Department [announced](#) that it would add four research institutes under a Chinese space agency, two under a state-owned military technology firm, and a satellite firm to the Entity List for acquiring and attempting to acquire U.S.-origin items in support of China's military modernization efforts. This activity is deemed contrary to national security and foreign policy interests under § 744.11(b) of the EAR.

BIS included a long list of aliases associated with the entities, bringing the possible names to screen against into the hundreds. These additions bring the number of sanctioned Chinese entities to approximately 600. For members of the Entity List, BIS imposes a license requirement for all items subject to the EAR, and will review license applications under a presumption of denial.

AI Chip Restrictions Get Real

On August 26, The Commerce Department informed NVIDIA Corporation of a new license requirement, effective immediately, for any future export to China (including Hong Kong) and Russia of the Company's A100 and forthcoming H100 integrated circuits. The license requirement also includes any future NVIDIA integrated circuit of comparable performance.

The day after disclosing the restrictions, Nvidia clarified that the subject chips will continue to be sold through its Hong Kong facility through September 2023, although the licensing requirement will stand. Rival AMD said it faced similar licensing restrictions, but the sales impact was not expected to be material.

[Reuters](#) notes "the curbs are likely to hit almost any major tech company running public clouds or advanced artificial intelligence training modules in the Asian country."

New Controls on Semiconductor Tools and Gas Turbine Tech

Commerce (BIS) issued an interim final [rule](#) August 12, establishing new export controls on four technologies supporting the production of advanced semiconductors and gas turbine engines that meet the criteria for emerging and foundational technologies under Section 1758 of the Export Control Reform Act (ECRA).

These four technologies are among the items that the 42 Participating States of the Wassenaar Arrangement agreed to control at the December 2021 Plenary. [Further information on other changes agreed to during the Wassenaar Arrange-

ment's December 2021 Plenary is available [here](#).]

"Technological advancements that allow technologies like semiconductors and engines to operate faster, more efficiently, longer, and in more severe conditions can be game changers in both the commercial and military context," said **Under Secretary of Commerce for Industry and Security Alan Estevez**. "When we recognize the risks as well as the benefits, and act in concert with our international partners, we can ensure that our shared security objectives are met, innovation is supported, and companies across the globe operate on a level playing field."

These four technologies are among the items that the 42 Participating States of the Wassenaar Arrangement agreed to control at the December 2021 Plenary

Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler said "We are protecting the four technologies identified in today's rule from nefarious end use by applying controls through a multilateral regime. This rule demonstrates our continued commitment to imposing export controls together with our international partners. Export controls are most effective when multilaterally imposed."

The four technologies covered by today's rule include **two substrates of ultra-wide bandgap semiconductors:** Gallium Oxide (Ga₂O₃), and diamond; **Electronic Computer-Aided Design (ECAD) software** specially designed for the development of integrated circuits with Gate-All-Around Field-Effect Transistor (GAAFET) structure; and **Pressure Gain Combustion (PGC) technology**.

- Gallium Oxide and diamond are materials that allow semiconductors that use them to work under more severe conditions, such as at higher voltages or higher temperatures.
- ECAD is a category of software tools used for designing, analyzing, optimizing, and validating the performance of integrated circuits or printed circuit boards. GAAFET technology approaches are key to scaling to 3 nanometer and below technology nodes.
- PGC technology has the extensive potential for terrestrial and aerospace applications, including rockets and hypersonic systems. BIS has added controls on development and production technology for combustors that are not described on the U.S. Munitions List.

OFAC issues Iran General License M-2 Education Services

"Authorizing the Exportation of Certain Graduate Level Educational Services and Software," permitting, on a time-limited basis, accredited graduate and undergraduate degree-granting U.S. academic institutions, including their contractors, to export additional services to those Iranian students who are eligible for non-immigrant classification under categories F (students) or M (non-academic students), and have been granted a nonimmigrant visa by the U.S. State Department, but are not physically present in the United States due to the COVID-19 pandemic. [GLM-2](#) is a renewal and replacement of GLM-1 issued in August of 2021.

YMTC Shoe to Drop?

Reuters [reports](#) that Biden Administration is planning to limit the export of American chipmaking equipment to memory chip makers in China including Yangtze Memory Technologies Co Ltd (YMTC).

The measure would target factories in China that manu-

facture advanced NAND chips used in smartphones, personal computers, and data centers. If implemented, the move would mark the first effort to use export controls to target Chinese production of memory chips without specialized military applications.

US Defense Contractor Plans "ITAR Free" Drone Subs

An offshore subsidiary of Anduril has agreed to build three prototype Extra Large Autonomous Undersea Vehicles for the Australian Navy, with the goal to develop mass production capability without sales being governed by the U.S. Department of State and ITAR, according to the CEO's statements to *Breaking Defense*. It is expected that sales of the vessels would be regulated by more liberal US Department of Commerce dual-use controls.

Founded in 2017, the venture-funded California firm has grown rapidly by adapting commercial technologies like sensor fusion, computer vision, edge computing, machine learning and artificial intelligence to battlefield applications.

SEE A PREVIEW OF

Mastering Deemed Exports

www.deemedexports.com

BIS publishes “Red Flags” list for Russia Sanctions

August 16th BIS Published a primer on “red flags” for export control evasion associated with the Russian sanctions, highlighting techniques and conduits commonly used. The department lists 16 specific technologies of interest, from Aircraft Parts and Equipment (ECCN 9A991) to Vacuum Pumps (ECCN 2B999). These commodities support the development of maritime technology, microelectronics, and other technologies that can be used to support Russia’s military and defense sector.

Illicit actors often attempt to procure EAR99 items – a category generally referring to low-tech consumer goods not specified on the Commerce Control List that do not require a license for export, re-export, or transfer to most destinations. EAR 99 transactions can still constitute a violation.

Red flags include the customary due diligence (entities with little to no web presence, the physical address does not exist, or it is residential), as well as connecting the dots: transactions associated with atypical shipping routes for a product and destination, or transactions involving freight-forwarding firms that are also listed as the product’s final end customer, especially items going to traditional Russian transshipment hubs.

BIS has identified 18 countries as transshipment points through which restricted or controlled exports have been known to pass before reaching destinations in Russia or Belarus. These include Armenia, Brazil, China, Georgia, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United

Arab Emirates, and Uzbekistan.

In some instances, controlled U.S. items may be legally exported to these and other jurisdictions as inputs to produce other finished goods. **However, further export to Russia or Belarus of those finished products and goods, potentially through additional transshipment points, may be prohibited.** BIS guidance on re-exports can be found here.

Aviation Sanctions Expand

BIS updated has its list of sanctioned aircraft flying in Russia and Belarus to include 25 Airbus models identified as apparently violating the EAR’s de minimis threshold for U.S. components. There are now a total of 183 aircraft identified on the list for apparent violations of U.S. export controls. “Today’s identification of 25 foreign-produced aircraft further degrades Russian airlines’ ability to operate their fleets of both U.S. and EU airplanes,” said Assistant Secretary of Commerce for Enforcement Matt Axelrod.

There are now a total of 183 aircraft identified on the list for apparent violations of U.S. export controls.

Any subsequent actions taken with regard to any of the listed aircraft, including, but not limited to, refueling, maintenance, repair, or the provision of spare parts or services, are subject to the prohibitions outlined in General Prohibi-



tion Ten of the EAR (Section 736.2(b)(10)). Any aircraft manufactured in the United States, or that is manufactured in a foreign country and includes more than 25 percent by value of U.S.-origin controlled content, is subject to a license requirement.

The Russia and Belarus Civil Aviation fleet includes more than 500 leased western-origin aircraft, according to [Cirium](#), with about 435 remaining in Russian hands. As compliant maintenance, repair and operating (MRO) resources dry up, expect continued enforcement actions in the MRO market, and heed Deputy Secretary Alan Estevez's advice given BIS Update attendees in June: "If I were you, I wouldn't fly on a Russian airplane."

Business aircraft remain a high-profile focus of sanctions activity. In August, a 16 year old Boeing Business Jet (737-7EM BBJ) became the latest target of the Office of Export Enforcement. Currently stored in Moscow, the aircraft was sanctioned for being flown there in March without the requisite BIS authorization.

Guryev's company PhosAgro, a major exporter of fertilizer remains free of sanctions, OFAC emphasized in FAQ 1075.

As part of the response to Russia's invasion of Ukraine, on February 24, 2022, BIS imposed a license requirement for the export or reexport to Russia of aircraft subject to the EAR.

On March 2, 2022, BIS also removed the availability of the Aircraft, Vessels, and Spacecraft (AVS) license exception for all aircraft registered in, owned, or controlled by, or under charter or lease by Russia or a national of Russia, meaning they must have BIS authorization for legal operation.

Flight records reflect that after the license requirement was put in place, the Lukoil-owned aircraft was reexported to Russia on one occasion without the requisite BIS authorization.

The aircraft flew from Dubai, United Arab Emirates to Moscow, Russia with a Lukoil official as a passenger. No re-export license was sought or obtained from BIS prior to the reexport of the aircraft.

Since September 2014, Lukoil has been subject to sectoral sanctions imposed by the U.S. Department of the Treasury's Office of Foreign Assets Control

OFAC issued more sanctions on Russian Elites, including A.G. Guryev, owner of Witanhurst, the second-largest estate in London after Buckingham Palace. His yacht, the 267 foot Alfa Nero, was sanctioned, but has disabled its AIS transponder and cannot be located, according to the announcement. **Guryev's company PhosAgro, a major exporter of fertilizer remains free of sanctions**, OFAC emphasized in [FAQ 1075](#).

OFAC also cited Magnitogorsk Iron & Steel (MMK), and two of the steel producer's subsidiaries, Russian investment company MMK-FINANS and Turkish steel manufacturer MMK Metalurji, as well as Viktor Rashnikov, the steel-maker's principal owner. Rashnikov's yacht, the 140 meter Ocean Victory last transmitted its location in the Maldives March 1st.

OFAC Rewrites Cyber Sanctions Rule

Treasury's Office of Foreign Assets Control (OFAC) is amending the Cyber-Related Sanctions Regulations, reissuing them in their entirety. This final rule replaces the regulations that were published in abbreviated form on December 31, 2015, and includes additional interpretive guidance and definitions, general licenses, and other regulatory provisions.

Originally issued April 1, 2015 under E.O. 13694, Treasury has authority to block property of any person determined be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located outside the United States that are likely to result in, or have contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States, and that have the purpose or effect of:

- (A) (harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- (C) (causing a significant disruption to the availability of a computer or network of computers;
- (D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or
- (E) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

Other actions include:

- (A) to be responsible for or complicit in theft of trade secrets through cyber-enabled means, likely to result in a significant threat to the national security,

- foreign policy, or economy of the United States; and
- (B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (1)(a)(ii) or (iii)(A) of amended E.O. 13694, or any person whose property and interests in property are blocked pursuant to amended E.O. 13694;
 - (C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to amended E.O. 13694; or
 - (D) to have attempted to engage in any of the activities described in subsections (1)(a)(ii) and (iii)(A)–(C) of amended E.O. 13694.

Cyber-Related CAATSA Provisions

Countering America's Adversaries Through Sanctions Act-Related Sanctions (CAATSA), established new sanctions authorities and exceptions, in addition to amending, modifying, or otherwise affecting certain Ukraine-related executive actions.

Title II of CAATSA required the imposition of sanctions with respect to, among others, activities of the Russian Federation that undermine cybersecurity and persons who knowingly provide financial services in support of activities that undermine cybersecurity.

OFAC is incorporating the prohibitions in section 224(a)(1) of CAATSA, as well as the exceptions listed in section 236 of CAATSA, into the Regulations. OFAC has already implemented section 10 of SSIDES, as amended by section 228 of CAATSA, in 31 CFR part 589.

OFAC anticipates incorporating the menu-based provisions of section 224(a)(2) of CAATSA into 31 CFR chapter V at a later date.

Subpart B detail the effect of transfers of blocked property in violation of the Regulations and set forth the requirement to hold blocked funds in interest-bearing blocked accounts.

Section 578.204 of subpart B provides that all expenses incident to the maintenance of blocked tangible property shall be the responsibility of the owners and operators of such property, and that such expenses shall not be met from blocked funds, unless otherwise authorized.

The section further provides that **blocked property may be sold or liquidated** and the net proceeds placed in a blocked interest-bearing account in the name of the owner of the property.

In subpart C of the Regulations, **new definitions are**

being added to other key terms used throughout the Regulations.

New § 578.405 explains that the prohibition on transactions with blocked persons in § 578.201 applies to **services performed by U.S. persons on behalf of a person whose property and interests in property are blocked**, as well as to services received by U.S. persons where the service is performed by, or at the direction of, a person whose property and interests in property are blocked.

OFAC is adding three new general licenses to the Regulations

Transactions otherwise prohibited by the Regulations but found to be consistent with U.S. policy may be authorized by one of the general licenses contained in subpart E of the Regulations or by a specific license issued pursuant to the procedures described in subpart E of 31 CFR part 501.

OFAC is redesignating the authorization for payments for legal services from funds originating outside the United States, and redesignating the authorization for emergency medical services.

OFAC is adding three new general licenses to the Regulations: a general license authorizing the investment and reinvestment of certain, a general license authorizing the official business of the U.S. government, and a general license authorizing certain official business of international entities and organizations.

General licenses and statements of licensing policy relating to this part also may be available through the **Sanctions Related to Significant Malicious Cyber-Enabled Activities** page on OFAC's website: www.treas.gov/ofac.

Because the Regulations involve a foreign affairs function, the provisions of E.O. 12866 of September 30, 1993, "Regulatory Planning and Review", and the Administrative Procedure Act (5 U.S.C. 553) requiring notice of proposed rulemaking, opportunity for public participation, and delay in effective date are inapplicable.

Landmark Crypto Sanction

Treasury's Office of Foreign Assets Control (OFAC) sanc-tioned virtual currency mixer "Tornado Cash", which has allegedly been used to launder more than \$7 billion worth of virtual currency since its creation in 2019. The money laundered by Tornado includes \$455 million stolen by the Lazarus Group, a North Korean (DPRK) state-sponsored hacking group that was sanctioned by the US in 2019.

Tornado Cash Sanctions Explained. FTI Consulting has published a readable explainer on the sanctions on the notorious crypto mixer and implications of the novel action: for the first time, Treasury has sanctioned a smart contract and a tool, substantially increasing the degree of technical engagement with the industry by the Department.

The Electronic Frontier Foundation has prepared a policy [paper](#) discussing ethical and constitutional questions raised by created by the action. The issues EFF is most concerned about arise from speech protections for software code and how they relate to government attempts to stop illegal activity using this code.

See OFAC's '[Sanctions Compliance Guidance for the Virtual Currency Industry](#)' and the 'Virtual Assets' section of the [2022 National Money Laundering Risk Assessment](#). OFAC FAQs on virtual currency are [here](#).

UK Sanctions Reporting Guide

Britain's Office of Financial Sanctions Implementation (OFSI) [posted](#) a primer on sanctions reporting obligations and how they can be met. UK financial sanctions legislation

sets out specific reporting obligations which requires certain individuals and entities ('relevant firms') to report to OFSI if: You know or have reasonable cause to suspect that an individual, entity or ship is a designated person; and if that designated person is a customer, and you hold frozen assets for them: their nature and amount or quantity; or you know or have reasonable cause to suspect that a person has committed an offence under financial sanctions regulations

You only need to report this information if, as a relevant firm, it comes to your knowledge while carrying out your business. Definitions of relevant firms can be found in the statutory instrument for each sanctions regime, which can be found [here](#).

In Germany, not one of the Russians targeted by European Union sanctions have declared their assets to German authorities, as required under Germany's sanctions law, the German government said, prompting calls for the transparency regime to be tightened. ([Reuters](#))

Subscribe Today to The Export Practitioner

Save \$100


The Export Practitioner **is the only publication devoted exclusively to reporting on U.S. export controls and trade sanctions.**

- Get fast, reliable news and analysis
- Avoid costly fines and penalties
- Move your export licenses quickly and smoothly



<https://www.exportprac.com/ht/d/Join/pid/6005>

Remember: Export Control Reforms Don't Mean Decontrol !!

 Cut out and return this money-saving coupon today.

YES, Begin my new subscription to **The Export Practitioner** for a full year (12 monthly issues) at the **Special Discount Price** of \$649 – a \$100 savings off the regular full price. I understand my subscription comes with a no-risk, money-back guarantee: If I ever feel it is not worth many times what I've paid, I may cancel at any time -- even the last day of my subscription -- and get a full, 100% refund!

I want to receive my issues ☐ Online or ☐ Print Copy by Mail

☐ Check Enclosed (payable to Gilston-Kalin Communications, LLC)
Charge Credit Card ☐ Visa ☐ MasterCard ☐ American Express

Card No. _____ Exp. Date ____/____/____

Name _____

Company _____

Address _____

City/State/Zip _____

Phone _____

E-Mail _____

3 Easy Ways to Subscribe

Online: www.exportprac.com
(Use coupon code: NS2022)

Phone: 703-283-5220

Mail to: Gilston-Kalin
Communications
P.O. Box 5325
Rockville, MD 20848-5325

