October 2023 | Vol. 37, No. 10

# EP THE EXPORT PRACTITIONER™

IN THIS ISSUE:



# Safe Harbors at Justice

*More rewards for voluntary self-disclosure*

# WELCOME TO YOUR NEW

# EXPORT PRACTITIONER™

## IN PRINT | VIA EMAIL | ONLINE


VISIT ONLINE AT EXPORTPRAC.COM

## FROM THE EDITOR:

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

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

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

## Share your thinking with the Export Practitioner community

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

**TO SUBSCRIBE, OR TO SUBMIT CONTENT:**
Contact Editor Frank Ruffing at fruffing@traderegs.com, or call 301-460-3060.

**Scan or Click For Our Top Stories:**

EP
THE EXPORT PRACTITIONER™
October 2023 | VOL. 37, NO. 10


SHREEKAR LATHIYA/ UNSPLASH

## FEATURE



## EXPORT CONTROLS



## ENFORCEMENT



## POLICY



## RULES & REGS



## SANCTIONS



**ON THE COVER:** Justice has sweetened inducements for self-disclosure. ADOBESTOCK

**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

FEATURE

**Department of Justice in Washington D.C. United States of America**

ORHAN ÇAM / ADOBE STOCK

# Monaco Announces Compliance Reforms

*Self-Disclosure, M&A Safe Harbors, Divestitures, Compensation*

Deputy Attorney General Lisa Monaco announced a "Department-wide Safe Harbor Policy" for voluntary self-disclosures of misconduct by acquirers in the mergers and acquisition process. She noted that the number of national security related corporate settlements had doubled in the past year.

"Our message should be clear: the tectonic plates of corporate crime have shifted. National security compliance risks are widespread; they are here to stay; and they should be at the top of every company's compliance risk chart."

In her speech to the Society of Corporate Compliance and Ethics October 4, Ms. Monaco declared "we are doubling down on clarity and predictability."

*[Her comments are reproduced below, lightly edited for brevity]*

If you've been paying attention to the policies we've implemented over the past two years, you've probably noticed that I talk a lot about empowering general counsels and compliance officers — to make the case in the board room and the c-suite for investments in compliance — and to make the case that investing in strong

compliance programs is good for business.

As compliance officers, you are on the front line of protecting your company and its shareholders, and in today's world, more and more frequently that means protecting national security.

Corporate enforcement is in an era of expansion and innovation. Over the past two years, we have engaged in corporate enforcement actions to protect national security in unprecedented numbers and unexpected industries.

We have adopted new tools to fashion tailored punishments and enhance the business case for robust compliance. And we have increased consistency, predictability, and transparency for all of you and the boardrooms you advise.

And we're not done. Some of the examples I'll share today make this case: Invest in compliance now or your company may pay the price — a significant price — later. Today, I'll discuss how we have advanced the fight against corporate crime and describe where we are going next:

• First, I will discuss the dramatic expansion of our corporate enforcement efforts in the national security realm, as we confront new risks that threaten our collective security.

• Second, I will discuss new tools we are using to penalize corporate misconduct and incentivize good corporate citizenship.

• Third, I'll announce our latest effort to promote voluntary self-disclosures: our new Mergers & Acquisitions Safe Harbor policy.

• Finally, I want to briefly preview areas where we see further opportunity for innovation and expansion.

Let me start by addressing the biggest shift in corporate criminal enforcement that I've seen during my time in government: the rapid expansion of national security-related corporate crime.

Today corporate crime intersects with our national security — in everything from terrorist financing, sanctions evasion, and the circumvention of export controls, to cyber- and crypto-crime.

And we are seeing new national security dimensions in familiar areas of corporate crime — from FCPA violations to intellectual property theft that affects critical supply chains and involves disruptive technologies.

Today, companies confront a complex geopolitical environment. Many companies are responding commendably. They are implementing sophisticated compliance controls to mitigate otherwise risky business lines and, where necessary, exiting markets that pose undue risk.

MATTHEW T. NICHOLS

**Lisa O. Monaco, Deputy Attorney General.**

But some companies have not kept pace with today's compliance challenges, and where those companies violate the law, we are holding them accountable.

**Let me highlight some notable examples.**

• Last October, in the first-ever corporate guilty plea for material support to terrorism, French cement firm Lafarge admitted to paying the Islamic State and an al Qaeda affiliate to protect its profits and gain market share. The company pleaded guilty to providing material support to terrorists and paid more than $775 million in penalties.

• In April of this year, British American Tobacco (BAT) entered into a deferred prosecution agreement (DPA), its subsidiary pleaded guilty, and the company paid more than $635 million for violating U.S. sanctions. BAT admitted to selling tobacco in North Korea, which, in turn, generated revenue that advanced North Korean nuclear programs.

• And last month, the Department announced the first-ever criminal resolution for sanctions violations from illicit sales and transport of Iranian oil. The shipping company, Suez Rajan Ltd, pleaded guilty, and the United States seized nearly one million gallons of contraband Iranian oil.

More and more of our corporate resolutions implicate our national security. In fact, already

**Continues on next page**

Continued from previous page

this year, the number of major national-security corporate resolutions has doubled compared to last year.

To meet this moment, we are adding more than 25 new corporate crime prosecutors in the National Security Division, including the division's first-ever Chief Counsel for Corporate Enforcement. And we are increasing by 40% the number of prosecutors in the Criminal Division's Bank Integrity Unit, which holds accountable financial institutions that violate U.S. sanctions and the Bank Secrecy Act.

Our message should be clear: the tectonic plates of corporate crime have shifted. National security compliance risks are widespread; they are here to stay; and they should be at the top of every company's compliance risk chart.

## Divestiture & Specific Performance

Now, we're not just expanding enforcement — we're developing new tools and remedies to punish and deter. This year, we have announced corporate criminal resolutions that, for the first time, include divestiture of lines of business, specific performance as part of restitution and remediation, and tailored compensation and compliance requirements.

For example, when the Antitrust Division recently announced DPAs with two pharmaceutical companies, Teva and Glenmark, we determined that a monetary penalty alone was not sufficient. Instead, the Department required the companies to divest a widely used cholesterol medicine that was a core part of the companies' price-fixing conspiracy.

This was the first time the Department required divestiture as part of a corporate criminal resolution. As another example of innovation, we are now employing specific performance as a new remedy. As part of the recent Suez Rajan resolution — not only did the company plead guilty, but it was required to transport almost one million barrels of contraband Iranian crude oil across the globe to the United States, where it was seized pursuant to court order.

**French cement firm Lafarge became the first-ever corporate guilty plea for material support to terrorism.**

FLORENCE PIOT / ADOBE STOCK


## Compensation Considerations

We are also keenly focused on the role compensation plays in guiding employee behavior. By rewarding compliance and deterring wrongdoing, a well-designed compensation program can align executives' financial interests with the company's interest in good corporate citizenship.

So earlier this year, I directed the Criminal Division to create a pilot program to jumpstart innovation in the design of compensation systems.

Under the pilot program, every Criminal Division resolution now requires companies to add compliance-promoting criteria to their compensation systems. These criteria are tailored to the company's existing compensation system to ensure integration with its compliance program.

The program is already bearing fruit, with incentive requirements included in several recent resolutions, such as those with Albemarle and Corficolombiana.

The pilot program also rewards companies that claw back or withhold incentive compensation from executives responsible for misconduct — or attempt to do so in good faith. For every dollar that a company claws back or withholds from an employee who engaged in misconduct — or a supervisor that knew of or turned a blind eye to it — the Department will deduct a dollar from the otherwise applicable penalty that the resolving company would pay.

Again, we are seeing positive early returns. For example, as part of last week's Albemarle resolution, the company received a clawback credit for withholding bonuses of employees who engaged in misconduct. **Not only did Albemarle keep the bonuses that would have gone to wrongdo-**

**ers, the company also received an offset against its penalty for the same amount.** That's money saved for Albemarle and its shareholders — and a concrete demonstration of the value of clawback programs.

Companies cannot wait to enact compliance-promoting compensation policies until they are in the government's crosshairs. Companies, their boards, and their compliance officers should be addressing how their compensation policies promote compliance today and should be assessing whether their clawback programs are fit for purpose and ready for deployment.

Compliance should no longer be viewed as just a cost center for companies. Good corporate governance and effective compliance programs can shield companies from enormous financial risks and penalties.

## Voluntary Self-Discolsures

DOJ's recent corporate enforcement actions, like the ones I mentioned a few minutes ago, illustrate the enormous gulf between outcomes for companies that do the right thing — that step up and own up — and companies that do the opposite.

To enhance transparency and predictability, I announced in March that every DOJ component engaged in corporate criminal enforcement now has a voluntary self-disclosure policy. So, when companies promptly disclose misconduct, fully and in a timely manner, they can take advantage of the programs' benefits in any type of case, in any part of the Department, and in any part of the country.

Encouraging companies to self-report misconduct can result in a virtuous cycle: by giving a path to resolution and declination to companies trying to do the right thing, we are able to identify and prosecute the individuals who are not. For example, earlier this year, we declined to prosecute Corsa Coal Corporation for FCPA violations, because the company timely and voluntarily self-disclosed the misconduct, remediated, cooperated, and disgorged the profits to the extent of its capability. Crucially, the company provided information about individual wrongdoers, including two former vice presidents who were charged criminally for their involvement in the scheme.

## New Mergers & Acquisitions Safe Harbor Policy

And this brings me to the next step when it comes to Voluntary Self Disclosure: our new Mergers & Acquisitions Safe Harbor Policy. In a world where companies are on the front line in responding to geopolitical risks — we are mindful of the danger of unintended consequences. The last thing the Department wants to do is discourage companies with effective compliance programs from lawfully acquiring companies with ineffective compliance programs and a history of misconduct. Instead, we want to incentivize the acquiring company to timely disclose misconduct uncovered during the M&A process.

Now, in 2008, the FCPA Unit published an opinion requested by the energy company Halliburton, in which the Department said it did not intend to take enforcement action against Halliburton for misconduct it self-disclosed and remediated post-acquisition within a certain timeframe. That opinion applied only to that transaction, however, and did not have broader application. Since then, some parts of the Department have addressed M&A transactions as part of their Voluntary Self Disclosure policies, though they differ from each other in approach.

So today, for the first time, we are announcing a Department-wide Safe Harbor Policy for voluntary self-disclosures made in the context of the mergers and acquisition process. Going forward, acquiring companies that promptly and voluntarily disclose criminal misconduct within the Safe Harbor period, and that cooperate with the ensuing investigation, and engage in requisite, timely and appropriate remediation, restitution, and disgorgement — they will receive the presumption of a declination.

To ensure consistency, I am instructing that this Safe Harbor policy be applied Department-wide. Each part of the Department will tailor its application of this policy to fit their specific enforcement regime, and will consider how this policy will be implemented in practice.

To ensure predictability, we are setting clear timelines. As a baseline matter, to qualify for the Safe Harbor, companies must disclose misconduct discovered at the acquired entity within six months from the date of closing. That applies whether the misconduct was discovered pre- or post-acquisition.

Companies will then have a baseline of one year from the date of closing to fully remediate the misconduct. Both of these baselines are subject to a reasonableness analysis because we recognize deals differ and not every transaction is the same. So,

*'... Some companies have not kept pace with today's compliance challenges, and where those companies violate the law, we are holding them accountable.'*

**Continued from previous page**

depending on the specific facts, circumstances, and complexity of a particular transaction, those deadlines could be extended by Department prosecutors. And of course, companies that detect misconduct threatening national security or involving ongoing or imminent harm can't wait for a deadline to self-disclose.

For transparency, we are making clear that aggravating factors will be treated differently in the M&A context. The presence of aggravating factors at the acquired company will not impact in any way the acquiring company's ability to receive a declination. Now, one question we have heard is how the Department will treat the acquired entity when an acquirer voluntarily self-discloses under the Safe Harbor Policy. Unless aggravating factors exist at the acquired company, that entity can also qualify for applicable VSD benefits, including potentially a declination.

Finally, misconduct disclosed under the Safe Harbor Policy will not affect any recidivist analysis at the time of disclosure or in the future. Put another way, any misconduct disclosed under the Safe Harbor Policy will not be factored into future recidivist analysis for the acquiring company.

Of course, this policy will only apply to criminal conduct discovered in bona fide, arms-length M&A transactions. The Safe Harbor does not apply to misconduct that was otherwise required to be disclosed or already public or known to the Department. Nor will anything in this policy impact civil merger enforcement.

So, for those advising boards and deal teams — here are the takeaways. We are placing an enhanced premium on timely compliance-related due diligence and integration. Compliance must have a prominent seat at the deal table if an acquiring company wishes to effectively de-risk a transaction.

By contrast, if your company does not perform effective due diligence or self-disclose misconduct at an acquired entity, it will be subject to full successor liability for that misconduct under the law. Our goal is simple: good companies — those that invest in strong compliance programs — will not be penalized for lawfully acquiring companies when they do their due diligence and discover and self-disclose misconduct.

And we are doubling down on clarity and predictability. Through careful due diligence and timely post-acquisition integration — alongside self-disclosure, remediation, disgorgement, and cooperation where warranted — acquiring companies can protect shareholders, promote compliance, and advance the goal of fighting corporate crime.

## So, what is next?

We are looking to apply our corporate enforcement principles across the entire Department, especially in areas implicating cybersecurity, tech, and national security.

The entire Department shares the same principles in both civil and criminal enforcement: (1) holding corporate and individual wrongdoers accountable, (2) incentivizing compliance, self-disclosure, remediation, and cooperation, and (3) deterring and penalizing repeat bad actors.

**You should expect more to come on this topic** as we continue to extend consistent, transparent application of our corporate enforcement policies across the Department, beyond the criminal context to other enforcement resolutions — from breaches of affirmative civil case settlements to violations of CFIUS mitigation agreements or orders.

Gone are the days when executives could view corporate enforcement matters as the cost of doing business. In this new era, corporate executives need to redouble time and attention to compliance programs, compensation programs, and diligence on acquisitions. Failing to do so can have dire consequences for companies, shareholders, and our nation.

The world is full of risks. Corporations, and by extension, all of you in corporate compliance, are on the front lines. Of course, your job is to protect your company, but in doing so, by focusing on robust compliance and by investing in good corporate governance, you are also protecting our national security. [11213]

*'Gone are the days when executives could view corporate enforcement matters as the cost of doing business.'*

PRACTITIONER PERSPECTIVE

# Ryan Fayhee: 'I'm one of the luckiest lawyers around'

**RYAN FAYHEE IS A PARTNER** *at Akin and is a former official and senior prosecutor with the U.S. Justice Department. Ryan's practice focuses on government and congressional investigations, crisis management, cross-border compliance, corporate governance, and white collar criminal defense.*

*Prior to private practice, Ryan served for 11 years in the DOJ, where he was a leading prosecutor handling complex cross border investigations and prosecutions affecting the national security and foreign policy of the United States, including espionage, sanctions and embargoes, arms proliferation, trade secret theft, cybercrime, corruption, and money laundering. Ryan also served in the National Security Division, where he most recently served as the principal DOJ attorney overseeing sanctions and export control prosecutions nationally. He also served on the inter-agency staff for CFIUS.*

*Ryan, you've got some history with us, and in the field, so we thought it'd be good to hear what's on your mind now. What would you like to tell your fellow practitioners, the attorneys who read our journal as well as the compliance executives, the folks in the trenches?*

Well, thanks. Glad to have the opportunity to connect. When I was a summer associate I had contributed to The Export Practitioner. I think it was in the summer of 2002. And then I took a little bit of a break from it because I would have been a law clerk and joined the Department of Jus-tice doing civil frauds litigation. Then the National Security Division opened up and then I was reacquainted with your publication around probably 2006.

## National Security Division Inception

I was one of the first new hires in the National Security Division days after it was established in 2006. The following year Steve Pelak came over from the US Attorney's Office and joined NSD as the first National Export Control Enforcement Coordinator. I hadn't really an idea what I was getting into, I thought I was going there to do espionage cases, (which I did a few of), but that

**Prior to private practice, Ryan Fayhee served for 11 years in the DOJ, where he was a leading prosecutor.**
SHANE NELSON

was really the beginning of what became the modern era of US export controls and sanctions enforce-ment becoming its is today.

**It wasn't as if I was sole the driver of that.** It had more to do with two big decisions. One was that the Department of Justice back in 2007 was go-ing to give these rules — which had been largely on the books since Thomas Jefferson's embargo on the British in The War of 1812 — more teeth. They'd been on the books, but I can't say that

**Continues on next page**

*'India, in many ways, is at the center of issues relating to both China and Russia, because of their appetite for oil.'*

**Continued from previous page**

there was any coordination around enforcement.

This was also happening in early post 9/11 era. There was this new Under Secretary at the Treas-ury Department, **Stuart Levy** who was a real creative thinker and trying to find the ways to target individual ma-lign conduct. It spun out of the counter terrorism measures that were being imposed and there became a particular focus on Iran.

All I can say is that I'm one of the luckiest lawyers around. I really loved and enjoyed my time I was able to be fairly entrepreneurial and brought priority prosecutions with close coordination and support from the regulatory agencies, Treasury, Commerce and State Departments.

One of the former assistant attorney generals over NSD is now deputy attorney general **Lisa Monaco** — she's quoted recently that "sanctions are the new FCPA." The truth is they already were. I would say, sanctions and export controls together, they were the new FCPA in 2007.

This experience and its many successes brought on the new era where we are today. The landscape today has changed entirely from that time where it really required a special initia-tive by the then deputy attor-ney general back in 2007 to add teeth to these measures.

**We see a broadening of these au-thorities to get into some unusual areas.** It's not a surprise that they are not purely focused on problematic relations for Iran or, you know, an embargo on Syria. Now you have these broader packages that that target corruption, and forced labor, murders in the Saudi em-bassy in Turkey. You could go on and on and on.

It's just really fascinating to me, the growth over the past ten years or so in the use of these rules.

## Justice Tomorrow

*Let's go back to the Justice Department. Syracuse University published a report that prosecution of white collar crimes is at an all-time low since tracking began during the Reagan administration, with prosecutions during the Obama Administration two and one half times the volumes last of year. The National Security Division has hired or plans to hire 25 new prosecutors. What can we expect from this?*

It's a good question. I mean in the in the National Security division we have seen an in-crease, a lot of increased activ-ity, around the so-called Klepto Capture task force. You know, targeting the luxury assets of Russian oligarchs and really trying to isolate them from the US financial system and the European financial system.

The other thing is that cases take a long time. I mean, even citing back to the Lafarge case. I did that Board-led investiga-tion beginning in 2016. The first news article that triggered it, in *Le Monde* was summer 2016. And the case in France, while many of those executives have been indicted, contin-ues. It had not been resolved by DOJ until late 2022. So that cut across three Presidential ad-ministrations.

It's not as if you can affect things as quickly as people per-ceive. Cross-border cases take a really, really long time. So you'd have to know a little bit around what's in the pipeline. But other than in that case, which again you know at least from the company's perspec-tive, the allegations were first out there 2016, you're really not seeing a ton of activity corpo-rate cases.

You know, I prosecuted the Schlumberger case that started in 2009. When it was finally re-solved in 2015, it was the largest non financial sanctions case in terms of total penalties, before ZTE came along. You know, these cases just take a really, really long time.

So I guess all I can say is there may be some in the pipe-line. It's really tough to judge, and with the new prosecutors, it'll take some time for them to get their get their traction.

*25 is a material change in the staffing over there, isn't it?*

In my old section, I don't be-lieve we had 25 lawyers. The question of how effective it'll be has to do with the leadership of the office and what they want

to do with it. Where are they recruiting the people from? Are these going to be brand new prosecutors doing this for the first time? Or are they going to be experienced prosecutors from US attorneys offices that have significant investigations and trial experience? Or are they going to come from some other source?

It's just really tough to know the answer to that question because, if they're brand new prosecutors, they're going to require serious training. This is not an easy field to learn on the fly because they're high profile cases.

I go back to what I think was was quite a success, this system back in 2007 where there was an intensive focus on coordinating the investigations of matters right across the United States, among law enforcement agencies, in particular the FBI, Commerce Department and Homeland Security Investigations, alongside some of the DoD investigative agencies like DCIS, NCIS, coordination there to make sure everybody's rowing in the same direction.

Influence in that process from the intelligence community, that tends to be on the leading edge in terms of creating priorities. And then coordination and referrals from an enforcement perspective at the regulatory agencies.

Also, its important to have the right people at Main Justice who can credibly team up with US attorney's offices around the country, because it's always a joint effort in the decentralized DOJ.


**The Schlumberger Oilfield Holdings Ltd. case started in 2009. When it was finally resolved in 2015, it was the largest sanctions case in terms of total penalties**

ADOBE STOCK / JHVEPHOTO

To really carry and elevate these cases and these investigations within that community, that was a good model. I don't think that that's the model that the department is currently pursuing, but I think that they would be well advised to reconsider how that was ultimately approached.

The other thing that we see, and I give good credit to, is **Matt Axelrod** at Commerce. Matt is somebody that did not have a deep experience with export controls. But he did have significant management experience at DOJ, as a prosecutor in the DAG's office. He's really stood out at raising the profile in a pretty meaningful way.

I'm not surprised by it. He's a very strong lawyer, very good guy. Good public servant. He's really done a tremendous job looking for ways to raise the profile of the matter, to make sure the resourc-ing and prioritizing is there as well, finding ways and avenues to search for new cases and so forth. It's pretty impressive.

*The cases don't originate from Justice for the most part, right? Doesn't the cop bring it to a prosecutor?*

Well, in a way, yes. That's the way a lot of Department of Justice cases start. But the truth is in this space you can really be entrepreneurial if you approach it the right way. I would argue actually that it's a joint effort, with law enforcement and the intelligence community, to find the right matters.

It isn't as if in a bank robbery or other accounting fraud, complex matters. There's opportunities for DOJ to be a little bit more on the leading edge in a way that it is not as traditional. Though having done this, created cases and then found myself without any law enforcement support at all, it's best when they do it together. [11241]

BIS

# Allies release updated list of priority items

**THE DEPARTMENT OF COMMERCE'S** Bureau of Industry and Security (BIS) released updates to its list of controlled "common high priority" items identified as critical to Russia's war effort following meetings with key members of the Global Export Control Coalition.

Since the onset of Russia's further invasion of Ukraine in February 2022, the United States and its international allies and partners have implemented a series of export controls that restrict Russia's access to the items it needs to sustain the war. While BIS's controls cover a vast array of items necessary to fuel Russia's war machine, certain items are more significant to Russian weaponry than others.

As part of this effort and in coordination with our partners in the United Kingdom, the European Union and Japan, **in July 2023 BIS published a list of 38 high priority items that Russia seeks to procure for its weapons programs. The list is divided into four tiers, ranked according to their relative degree of criticality.**

In coordination with partners, **BIS has added seven new Harmonized System (HS) codes to the list**, including bearings needed for heavy vehicles or other machinery and antennae used for navigation systems.

**Additionally, Tier 3 has been divided into mechanical and non- mechanical items to provide greater clarity.**

As published in our previous guidance involving the nine HS codes in Tiers 1 and 2 of highest priority, exporters and reexporters are strongly encouraged to conduct due diligence when encountering the listed HS codes to identify possible third-party intermediaries and attempts at evasion of U.S. export controls.

**BIS has implemented stringent export controls that restrict Russia's access to items that it needs to sustain its attack on Ukraine.**

ADOBE STOCK / MISU

## Russia Export Controls

Since February 24, 2022, the Department of Commerce's Bureau of Industry and Security (BIS) has implemented a series of stringent export controls that restrict Russia's access to the technologies and other items that it needs to sustain its brutal attack on Ukraine. These restrictions also apply to Belarus in response to its substantial enabling of Russia's destabilizing conduct.

## List of Common High Priority Items

The list is divided into four tiers.

- **Tier 1:** Items of the highest concern due to their critical role in the production of advanced Russian precision-guided weapons systems, Russia's lack of domestic production, and limited global manufacturers.
- **Tier 2:** Additional electronics items for which Russia may have some domestic production capability but a preference to source from the United States and its partners and allies.
- **Tier 3.A:** Further electronic components used in Russian weapons systems, with a broader range of suppliers.
- **Tier 3.B:** Mechanical and other components utilized in Russian weapons systems.
- **Tier 4:** Manufacturing, production and quality testing equipment for electric components, circuit boards and modules.

Within this list, BIS has prioritized the nine HS codes in Tier 1 and Tier 2 — covering items such as integrated circuits and radio frequency (RF) transceiver modules — that have extensive commercial applications but have also been found in Russian missiles and drones on the battlefield in Ukraine. [11136]

# BIS Suggests End User Certification for EAR Compliance

**THE DEPARTMENT OF COMMERCE'S** Bureau of Industry and Security (BIS) has published new best practice guidance for industry to help prevent items that are considered the most significant to Russian weaponry requirements from being diverted for use in Russia's war against Ukraine.

**The September 28 guidance recommends that exporters and reexporters of these highest priority items seek written assurances of compliance from their customers to help prevent diversion.**

In their September 14 guidance BIS, together with allies and partner countries, identified forty-five Harmonized System (HS) codes covering controlled items at heightened risk of being diverted illegally to Russia because of their importance to Russia's war efforts.

Of these, BIS has prioritized nine HS codes as the most significant to Russian weaponry requirements (the Highest Priority Items List).

Given the heightened threat resulting from Russia's continued attempts to evade U.S. export controls through third countries for which a BIS export license is generally not required, it is recommended that, at least for transactions involving these nine "Highest Priority Items" with parties in countries outside of the Global Export Controls Coalition (GECC), exporters seek assurances of compliance with U.S. export controls.

It is a best practice to receive these assurances in writing, for example, through a signed certification statement.

**BIS has identified the following information and assurances** that can help prevent the diversion of Highest Priority Items to Russia through non-GECC countries. For exporters that already are using customer certifications or end-user statements, the suggestions below are not meant to replace what you have already determined best mitigates diversion risk.

BIS does, however, encourage you to consider whether it's worth adding any of the suggestions to your existing documentation to help prevent diversion through third countries to Russia.

• **Full name and address** of the non-GECC customer, line of business, website address, and role in the transaction (i.e., purchaser, intermediate consignee, ultimate consignee, or end user). For new customers, request a copy of the business license.

• **Activity the customer intends to take with the item:** Consumed, Transformed into a different item (e.g., through further processing, integration, or incorporation), Maintained for stock, including the likelihood for reexport v. transfer (in-country), Resold with a specification as to who the next customer is (name and address)

• If the customer is not the end user, the **name and address of the known end user.**

• List of items covered by the transaction and confirmation from the customer that the item requires a license if exported or reexported to Russia or Belarus.

• **Attestation that the customer will comply with the Export Administration Regulations (EAR)** and flow-down these EAR requirements to its customers and other parties to the subsequent reexport or transfer (in-country) transaction to:

• Ensure that before reexporting or transferring (in-country) the item, **subsequent parties to a reexport or transfer (in-country) transaction will be screened** against the U.S. Consolidated Screening List6 and comply with any restrictions related to any such transaction parties.

• Not providing the item for end use by or to end users of the military, intelligence, or national police of Belarus or Russia.

• Not providing the item for end uses or to end users tied to nuclear weapons, chemical and biological weapons, or missiles or unmanned aerial vehicles capable of a range of at least 300 kilometers (or when such range is unknown).

• Not providing the item for ultimate end use in Belarus or Russia or temporarily occupied regions of Ukraine and covered regions of Ukraine pursuant to Part 746.6 of the EAR.

• Certification by the customer, including name, title, phone number, email address, date, and signature. [11203]

RAPTAC

# Regulations & Procedures Roundup

**THE COMMERCE DEPARTMENT'S** Bureau of Industry and Security Regulations and Procedures Technical Advisory Committee met September 12th, with little news, but steady progress on the rulemaking front.

The meeting began with a presentation on repressive technologies by **Annie Boyajian**, **VP Policy & Advocacy** with the human rights organization **Freedom House**, concluding with the following ask:

**"We would strongly urge the advisory Committee to recommend to Commerce a formal mechanism of ongoing engagement with civil society organizations and human rights defenders.** The Department of State and Department of Treasury do this, particularly with global Magnitsky sanctions, but this has also evolved into engagement on other targeted sanctions.

## BIS Review

Hillary Hess, Director, Regulatory Policy Division at BIS reviewed the summer's rulemaking activity, including:

• Additions to the entity list involving entities from Greece, Hungary, Ireland, and North Macedonia on July 19th.

• Expansion of nuclear nonproliferation controls on China and Macau as of August 14th in response to the military-civil fusion strategy, with a focus on preventing misuse of dual-use items and nuclear forces.

• An update on August 18th to the Nuclear Suppliers Group controls based on meetings held in June 2019 and June 2022.

• Revisions to the unverified list (UVL) on August 22nd where several entities were removed, primarily because they complied with end-use check requirements.

• An adjustment to the temporary denial order rules on August 29th, providing an option for renewal under certain circumstances for a period not exceeding one year.

As well as the following updates:

"The **interim rule on semiconductors** we published last October, we're looking at updates to it."

"We continue to be **particularly engaged with allies on Russia** and staying coordinated. Certainly our end user review committee is constantly working."

**US persons controls.** "Congress used the NDAA to tweak the wording, so we're working on that [implementation in the EAR.] By inserting the words and punctuation "security, or" before "intelligence" Congress gave **BIS authority to create and impose controls on the activities of U.S. persons, wherever located, in "support" of "military, security, or intelligence services" — even when all the underlying items at issue are not subject to the EAR.**

**Standards Body Participation:** September 9, 2022 BIS published an interim final rule [87 FR 55241] amending the EAR to authorize the release of specified items subject to the EAR without a license when that release occurs in the context of a "standards-related activity," as defined in the rule. "We got a lot of very helpful comments on it. We've been through the comments, and we are in the process of preparing to address those. We would like to have that out in 2023, still in the calendar year. It will then have to clear other agencies. It will be significant. It's been a real education process, between standards & controls people. We've certainly raised awareness."

## Treasury Conflict Rooted Out

Export Control Legend **Bill Root** brought to the Committee's attention a regulatory nuance of vital import. The Treasury Department's proposed "Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern" could create a material conflict with Commerce export controls.

*"I think the important issue is, does Treasury intend to have a separate definition for the national security technologies and products that are involved in the investment executive order?*

*"It would be very confusing if Treasury and Commerce were operating on two different definitions of just six words: technologies, products, Semiconductor Microelectronics. Quantum, and artificial intelligence. Those are the keywords in both the Executive order and the ANPRM, and although Treasury does not explicitly state, it's going to have a definition which is different from commerce on these six points."* [11068]

RAPTAC

# Census Updates Country of Origin and Routed Exports

**GERRY HORNER,** Chief of the Trade Regulations Branch at the US Census Bureau, gave the committee an update on two Notices of Proposed Rulemaking: the **Routed Export Transaction rule**, published prior to 2019, and the **Country of Origin data element,** released in December 2021.

## Country of Origin Data Element

Starting with the country of origin rule: this rule was introduced in December 2021 to incorporate a country of origin data element when the foreign domestic origin indicator is in the Automated Export System [86 FR 71187]. Our Trade Regulations Branch has spent significant time reviewing the comments. Notably, 52% of the total comments were centered on the burdens introduced by the rule.

Given the significant concerns from industry stakeholders about potential costs and current unpreparedness, we are considering three potential paths:

- Withdrawing the proposed rule.
- Gradual implementation.
- Analyzing what aspects would be most beneficial for federal adoption.

**The core motive behind this data element is to determine its statistical benefits for the U.S. Census Bureau.** We're examining whether there's a genuine need to release data at the country of origin level.

The emphasis on the foreign component's value in an export is another area of discussion. This criterion differs from other existing systems, like the WTO system or the tariff shift rule. Several feedback points also highlighted the complexities arising from commingled origins. Notably, the U.S. remains one of the few countries not collecting country of origin data on exports.

## Routed Export Transaction: Notice of Proposed Rule Update

The last time we openly provided an update on this was during the BIS update in 2019. Currently, our regulations, particularly the foreign trade regulation, define a routed transaction as one where the firm principal facilitates the export and prepares and files the electronic export information. Conversely, the EAR speaks about the

**Continues on next page**

**The country of origin rule was introduced to incorporate a country of origin data element when the foreign domestic origin indicator is in the Automated Export System.**

ADOBE STOCK

**Continued from previous page**

Foreign Principal Party in Interest (FPI) facilitating the export from the U.S. The EAR further details what routing is and the conditions where the exporter authorization is granted to an agent in the US, working on behalf of the foreign principal.

The proposed rulemaking [84 FR 67255] aims to embed the routing section within the foreign trade regulations, ensuring both sets of routed export transaction regulations align with each other. Our plan involves defining two types of routed transactions:

- The U.S. principal party in interest remains the exporter.
- The agent is granted authority under routing to assume the role of export control, export determination, and to apply for a license if required.

This is crucial for the Census Bureau since we establish the requirements for ACE reports. Additionally, the new notice of proposed rulemaking will standardize terms like "ultimate consignee," "authorized agent," and "standard export transaction." Presently, while we mention "routed export transaction," we fail to denote its opposite as a "standard transaction." This consistency should be mirrored in both regulations. Other roles, such as the foreign principal party in interest and buyer definitions, need uniformity.

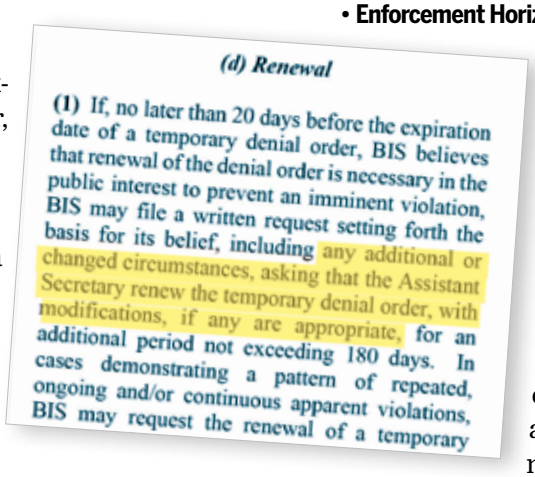
Our goal is to embed these definitions into the foreign trade regulations to standardize what an "end user" means and to define a foreign individual eligible to be a US PPI when they enter the US and procure goods for export. [11072]

BIS

# Denial Orders Up to One Year

**THE FINAL RULE** issued by the Bureau of Industry and Security (BIS), Department of Commerce, presents a modification to the existing Export Administration Regulations (EAR) concerning the renewal of temporary denial orders (TDOs). Under the newly adopted § 766.24(d)(1), BIS is now permitted to request the Assistant Secretary for Export Enforcement to extend an existing TDO for up to one year, a substantial extension from the previous 180-day limit.

This enhanced provision is triggered in cases where a subject party has exhibited a pattern of repeated and ongoing violations of the EAR, thereby justifying the need for a more protracted control mechanism.



*(d) Renewal*

(1) If, no later than 20 days before the expiration date of a temporary denial order, BIS believes that renewal of the denial order is necessary in the public interest to prevent an imminent violation, BIS may file a written request setting forth the basis for its belief, including any additional or changed circumstances, asking that the Assistant Secretary renew the temporary denial order, with modifications, if any are appropriate, for an additional period not exceeding 180 days. In cases demonstrating a pattern of repeated, ongoing and/or continuous apparent violations, BIS may request the renewal of a temporary

Key distinctions in this new regulation include:

- **Standard for Extension:** Unlike the previous regime that centered on imminent violations, the extended renewal requires BIS to substantiate that the subject party has been engaged in a continuous pattern of violations.
- **Fact-Based Evidence:** The new requirement obliges BIS to provide concrete facts of past violations in addition to forecasting imminent violations.
- **Legal Foundation:** The rule makes editorial adjustments to reflect the EAR's current statutory basis, replacing references to the outdated Export Administration Act (EAA) with the Export Control Reform Act (ECRA).
- **Enforcement Horizon:** If a request for an extended TDO renewal doesn't meet the new standard, the existing 180-day extension provision remains applicable, subject to BIS demonstrating its necessity in the public interest

**This final rule does not change the current language** set forth in the first sentence of paragraph (d)(1), which allows BIS to request the renewal of a TDO for a period of 180 days by demonstrating that such a renewal is necessary in the public interest to prevent an imminent violation of the EAR.

Rather, this final rule allows BIS to request the renewal of a TDO for an extended period by demonstrating that a party that is subject to an existing TDO has engaged in a pattern of repeated, ongoing and/or continuous apparent violations of the EAR. [10992]

FINCEN

# Report Finds Export Control Evasion

**THE FINANCIAL CRIMES ENFORCEMENT** Network (FinCEN) revealed a Financial Trend Analysis (FTA) concerning potential evasion of Russia-related export controls, based on Bank Secrecy Act (BSA) reports amounting to nearly $1 billion in suspicious activity.

After Russia invaded Ukraine, FinCEN and the Bureau of Industry and Security (BIS) issued alerts urging U.S. financial institutions to monitor potential Russian attempts to bypass U.S. export controls. This collaboration with financial entities has led to significant leads on potential Russia-related export control violations.

**BIS utilizes data from BSA reports to instigate new investigations and support ongoing ones.** This data assists in identifying parties in Russia and third countries undermining U.S. national security and foreign policy, resulting in their designation on the Entity List and imposition of license requirements according to the Export Administration Regulations, thereby obstructing foreign parties from evading BIS export controls.

## The FTA revealed several trends in BSA reporting:

• Post-invasion transactions indicate intermediary countries possibly procured U.S.-origin goods for Russian end-users.

• Transactions link trade activity, likely involving sensitive items, between Russian end users and jurisdictions like China, Hong Kong, and Turkey.

• Predominantly, companies in the dataset are associated with the electronics industry, possibly facilitating Russian export control evasion.

• Industrial machinery companies may also be supplying equipment to Russia.

Specific instances indicating potential evasion of Russia-related export controls include:

## Fluid Transfer System Components Company

• A U.S. company manufacturing fluid transfer system components received wires from Russian entities for potential purchases from December 2021 to October 2022.

• Between October 2022 and January 2023, the same company began receiving purchase wires from a Central Asia-based company, hinting at a potential attempt to sidestep Russia-related export controls.

## Underwater Technology Company

• A U.S.-based underwater technology entity returned funds to a Russian ecological center between April and June 2022.

• These funds were originally from a Hong Kong subsidiary of a Chinese entity listed on the BIS Entity List. This Chinese entity was designated for assisting Russia in monitoring submarines. The Hong Kong subsidiary specializes in supplying hydrographic survey and ocean mapping instruments.

## Intermediary Companies

• Companies located in intermediary countries seem to be buying U.S.-origin goods on behalf of Russian end-users.

• Primarily, these intermediary companies were situated in China and Hong Kong. However, other countries like Belgium, Germany, Singapore, Turkey, UAE, UK, among others, also seemed involved, hinting at possible transshipment activities and origination of goods payments.

## UAE-Based Companies Network

• BSA data pinpointed a group of companies based in the UAE, with some banking in Hong Kong. This network moved items, including electronics and computer components, from countries like China, South Korea, and the U.S. to Russia through third countries. Transactions were detected from Russia to the UAE between January 2020 and April 2023.

## Central Asia-Based Companies

• Companies situated in Central Asia, often affiliated with Russia-based entities or subsidiaries thereof, sourced goods like electronic components or aircraft parts from suppliers that had previously transacted with related Russian companies.

## Disparate Lines of Business

• Some BSA reports indicated potential evasion concerning transactions between Russia-associated entities and entities with varying business lines, where the exact purpose of the payments was ambiguous.

• One such example includes a UAE-based electronic products retailer, suspected of buying goods for Russian entities. This retailer conducted transactions with companies across multiple countries, such as Azerbaijan, the British Virgin Islands, Estonia, Kazakhstan, Kyrgyzstan, Russia, and Serbia. These companies spanned various unrelated business sectors.

These patterns and specific transactions underscore the intricate and often concealed strategies employed by entities to potentially circumvent Russia-related export controls. [11044]

# Pratt & Whitney Parts Operation Cited in Antiboycott Case

Bureau of Industry and Security (BIS) imposed a civil penalty of $48,750 against Pratt & Whitney's aftermarket parts division to resolve 13 violations of the antiboycott provisions of the Export Administration Regulations (EAR) (antiboycott regulations)

**PWCS voluntarily disclosed the conduct to BIS, cooperated with the investigation by BIS's Office of Antiboycott Compliance (OAC), and took remedial measures after discovering the conduct at issue, all of which resulted in a significant reduction in penalty.**

"Today's enforcement action highlights the need for robust antiboycott training and compliance procedures," said **Assistant Secretary for Export Enforcement Matthew S. Axelrod.** "Those who do business with boycotting countries need to train employees to recognize problematic boycott language and to report it to BIS, even when they do not take the requested action."

PRATT & WHITNEY

**PW4000 112-inch engine**

## BIS Case Background

As part of the settlement with BIS, PWCS admitted to the conduct set forth in the Proposed Charging Letter, which alleged 13 violations of Section 760.5 of the EAR (Failing to Report the Receipt of a Request to Engage in a Restrictive Trade Practice or Foreign Boycott Against a Country Friendly to the United States).

**Specifically, between May 2019 and March 2020, on thirteen occasions, PWCS received a request from Qatar Airways, a customer in Qatar, to refrain from importing Israeli-origin goods into Qatar in fulfillment of purchase orders from Qatar Airways.** PWCS failed to report to BIS the receipt of these requests, as required by Section 760.5 of the Regulations.

## Additional Information

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

In addition, U.S. persons must report to OAC their receipt of certain boycott-related requests. Reports may be filed electronically or by mail on form BIS 621-P for single transactions or on form BIS 6051P for multiple transactions involving boycott requests received in the same calendar quarter.

U.S. persons located in the U.S. must postmark or electronically date stamp their reports by the last day of the month following the calendar quarter in which the underlying request was received.

For U.S. persons located outside the U.S., the postmark or date stamp deadline is the last day of the second month following the calendar quarter in which the request was received. [11022]

# 3M Settles Iran Sales Case

**THE U.S. DEPARTMENT** of the Treasury's Office of Foreign Assets Control (OFAC) announced a $9,618,477 settlement with 3M Company ("3M").

3M has agreed to settle its potential civil liability for 54 apparent violations of OFAC sanctions on Iran that arose from its subsidiary's sale of reflective license plate sheeting to an Iranian entity controlled by the Iranian Law Enforcement Forces. Between September 2016 and September 2018, 3M East AG sold 43 orders of this product to a reseller with knowledge that it was destined for a customer in Iran.

This case involving 3M Gulf and the subsequent sanctions violations can be summarized as follows:

## Background

• In 2015, 3M Gulf intended to sell Reflective License Plate Sheeting (RLPS) to a German company, believing the sheeting would be used to produce license plates for Iran.

• In January 2016, the JCPOA took effect, along with General License H (GL H). GL H allowed foreign subsidiaries of US companies to engage in certain Iran-related transactions but with notable exclusions, including prohibiting transactions with Iranian military or law enforcement agencies.

## The Violations

In March 2016, a proposal was submitted indicating that the RLPS would be used by a German company to produce license plates for "transport authorities in Iran."

• Despite internal guidance and new procedures set by 3M, 3M Gulf's plan deviated from the original proposal.

• In April 2016, the German reseller informed 3M Gulf that it would sell the RLPS to Bonyad Taavon Naja (BTN) in Iran, an entity connected to Iran's Law Enforcement Forces (LEF). This change was not properly reported.

• Despite concerns and warnings from multiple channels, the sales went through. From September 2016 to September 2018, 43 shipments were made.

## Consequences

• A US employee, against guidelines, had significant involvement in the sales to Iran, further violating sanctions.

• When the sales were discovered, 3M voluntarily disclosed the violations to OFAC, took action against the involved employees, and put new compliance measures in place.

• OFAC determined that 3M Gulf's actions were an "egregious case" of violations.

• The potential maximum penalty was $27,481,363, but given mitigating factors, 3M settled with OFAC for $9,618,477.

## Lessons

• This situation emphasizes the need for companies to have robust, effective, and dynamic sanctions compliance programs. Proper oversight, clear communication, and active monitoring are vital, especially when transacting with high-risk areas.

• Even with a compliance program in place, companies must be vigilant and ensure that employees adhere to established procedures. Changes in the sanctions landscape can introduce nuances that require heightened scrutiny.

• The case also illustrates the importance of clear and effective processes, especially when exploring new business opportunities in high-risk areas. [11140]

# BIS Nabs Russian Component Dealers

**COMMERCE'S BUREAU OF INDUSTRY** and Security (BIS) issued a Temporary Denial Order (TDO) against three individuals and four companies implicated in illicitly supplying the Russian military with U.S.-sourced micro-electronics having significant military applications.

The TDO represents a robust form of civil sanction, precluding the concerned parties from any activities associated with U.S. exports as defined under part 764 of the Export Administration Regulations (EAR). Issued for a renewable 180-day period, the order is intended to curb imminent violations of the EAR.

## Case Background

The individuals and entities targeted by the TDO are implicated in a procurement network sourcing restricted U.S. micro-electronics for the

**Continues on next page**

**Continued from previous page**

Russian military, especially components integrated into Russian military hardware used in the ongoing conflict with Ukraine. The network operated through shell companies and complex routing to evade U.S. export controls.

Arthur Petrov is linked with Astrafteros Technokosmos LTD, a Cyprus-registered shell company, and also operates within Electrocom VPK, a Russian military supplier. Zhanna Soldatenkova, residing in Russia, works for Electrocom VPK and uses Ultra Trade Service, a Latvian third-party distributor, for transshipping U.S. electronics to Russia. Ruslan Almetov, another Russian national, serves as the General Director of Electrocom VPK and operates Juzhoi Electronic, a shell company based in Tajikistan.

To execute the scheme, controlled U.S. microelectronics were procured through various channels, including Petrov's Astrafteros, and then transshipped through third-country entities. In total, the network acquired and sent over $225,000 worth of controlled U.S. electronics to Russia without ever applying for a U.S. export license.

In parallel, Arthur Petrov is also facing criminal charges for export control violations, smuggling, wire fraud, and money laundering, filed by the U.S. Department of Justice in the Southern District of New York. Petrov was arrested in Cyprus on August 26, 2023, and is currently in custody pending extradition proceedings. [11002]

# Russian Arrested in Hong Kong Dual Use Ruse

**A RUSSIAN CITIZEN WHO HAS RESIDED** in Hong Kong, was charged in connection with conspiring to defraud the U.S. and with smuggling, wire fraud, and money laundering offenses based on his alleged participation in a scheme to unlawfully procure U.S.-sourced, dual-use microelectronics with military applications on behalf of end users in Russia.

According to the complaint, Maxim Marchenko, 51, employed a web of shell companies as part of an overseas smuggling ring to ship dual-use U.S. technology with military applications to Russia in contravention of U.S. law.

"As alleged, Maxim Marchenko participated in an illicit procurement network that provided military grade microelectronics to end users in Russia," said U.S. Attorney Damian Williams for the Southern District of New York.

"Following Russia's unjust invasion of Ukraine, Marchenko and his co-conspirators are alleged to have used shell companies and other deceptive measures in order to secure U.S.-manufactured microelectronics, with applications including in rifle scopes, night-vision goggles, thermal optics, and weapon systems, for use by Russians. This office will relentlessly pursue those who seek to flout U.S. law in order to sup-


**According to court documents, Maxim Marchenko, a Russian national, operates several Hong Kong-based shell companies**

ADOBE STOCK /F11PHOTO

ply Russia with military technology."

"Disrupting the efforts of facilitators and procurement agents like Marchenko, who use their skills and connections to advance the agenda of the Russian war machine, is one of the most important priorities of this task force. Today's arrest should serve as another reminder that we will leverage and deploy every tool to bring these criminals to justice," said Task Force KleptoCapture Co-Director David Lim.

According to court documents, Maxim Marchenko is a Russian national who resides in Hong Kong and operates several Hong Kong-based shell companies, including Alice Components Co. Ltd. (Alice Components), Neway Technologies Limited (Neway) and RG Solutions Limited (RG Solutions).

Marchenko and two co-conspirators (CC-1 and CC-2), who are also Russian nationals, have operated an illicit procurement network in Russia, Hong Kong and elsewhere overseas.

## About the scheme

This procurement network has fraudulently obtained from U.S. distributors large quantities of dual-use, military grade microelectronics, specifically OLED micro-displays, on behalf of Russia-based end users.

To carry out this scheme, Marchenko, CC-1 and CC-2 used shell companies based in Hong Kong and other deceptive means to conceal from U.S. Government agencies and U.S. distributors that the OLED micro-displays were destined for Russia.

The technology that Marchenko and his co-conspirators fraudulently procured have significant military applications, such as in rifle scopes, night-vision googles, thermal optics and other weapon systems.

To perpetrate the scheme, Marchenko and other members of the conspiracy acquired the dual-use OLED micro-displays from U.S.-based distributors using Marchenko's Hong Kong-based shell companies, including Alice Components, Neway and RG Solutions.

Members of the conspiracy, including Marchenko, procured these sensitive microelectronics by falsely representing to the U.S. distributors (who, in turn, are required to report to U.S. agencies) that Alice Components was sending the shipments to end users located in China, Hong Kong and other countries outside of Russia for use in electron microscopes for medical research.

In reality, the OLED micro-displays were destined for end users in Russia. Marchenko and other members of the conspiracy concealed the true final destination (Russia) from U.S. distributors for the purpose of causing false statements to the U.S. agencies.

To conceal the fact that these OLED micro-displays were destined for Russia, Marchenko and other members of the conspiracy worked together to transship the illicitly procured OLED micro-displays by using pass-through entities principally operated by Marchenko in third countries, such as Hong Kong.

Marchenko then caused the OLED micro-displays to be shipped to the ultimate destination in Russia using, among other entities, a freight forwarder known to provide freight forwarding services to Russia.

In addition, Marchenko and other members of the conspiracy used Hong Kong-based shell companies, principally operated by Marchenko, to conceal the fact that payments for the OLED micro-displays were coming from Russia.

In total, between in or about May 2022 and in or about August 2023, Marchenko's shell companies funneled a total of more than $1.6 million to the U.S. in support of the procurement network's efforts to smuggle the OLED micro-displays to Russia.

## About the charges

Marchenko is charged with conspiracy to defraud the U.S., which carries a maximum penalty of five years in prison; conspiracy to commit money laundering, which carries a maximum penalty of 20 years in prison; conspiracy to smuggle goods from the U.S., which carries a maximum penalty of five years in prison; money laundering, which carries a maximum penalty of 20 years in prison; smuggling goods from the U.S., which carries a maximum penalty of 10 years in prison; conspiracy to commit wire fraud, which carries a maximum penalty of 20 years in prison; and wire fraud, which carries a maximum penalty of 20 years in prison.

A federal district court judge will determine any sentence after considering the U.S. sentencing guidelines and other statutory factors. [11112]

# BRIEFS

## Settlement for Rocket Propellant Sales to China

➤ The State Department charged Island Pyrochemical Industries Corp. with three violations of the Arms Export Control Act and and the International Traffic in Arms Regulations on Aug. 25.

In a letter from Jae Shin, Director of the Defense Trade Controls Compliance Bureau of Political-Military Affairs, the State Department charged Island, maker of "rocket propellants and precursor chemicals used in explosive ordnance" with: 1) Brokering Without Obtaining the Required License or Written Approval; 2) False Statement, Misrepresentation, or Omission of a Material Fact on DSP-5 License Applications; Respondent Seriously Violated the ITAR

According to the State Department, Island brokered with a Chinese company without its approval. The Department also charged Island with "falsely listing itself as the seller and source of the defense article on a DSP-5 license application" in 2015. [10996]

## Petrobras Graft Charges Updated

➤ A federal grand jury in the District of Connecticut returned a superseding indictment charging a Connecticut-based oil and gas trader for his role in an alleged scheme to pay bribes to Brazilian officials to win contracts with Brazil's state-owned and state-controlled energy company, Petróleo Brasileiro S.A (Petrobras).

According to court documents, Gary Oztemel, 66, was the owner and president of Oil Trade & Transport S.A. (OTT) and the owner of Petro Trade Services Inc. (Petro Trade), both of which operated in Connecticut. From 2010 through 2018, Gary Oztemel, his brother Glenn Oztemel, Brazil-based intermediary Eduardo Innecco, and others allegedly paid bribes to Petrobras officials for their assistance in helping two Connecticut-based trading companies and OTT obtain and retain business with Petrobras.

As part of the scheme, a Petrobras official provided Gary Oztemel, Glenn Oztemel, Innecco, and others with confidential information regarding Petrobras' fuel oil business. Gary Oztemel also used his company Petro Trade to conceal the proceeds of the scheme.

In addition to the original charges, the superseding indictment charges Gary Oztemel with conspiracy to violate the Foreign Corrupt Practices Act (FCPA), conspiracy to commit money laundering, and two counts of money laundering. If convicted, he faces a maximum of five years in prison for the conspiracy to violate the FCPA charge, a maximum of 20 years in prison for money laundering conspiracy and the first money laundering charge, and a maximum of 10 years in prison for the second money laundering charge. [11005]

## Steel Traders Guilty in Sanctions Plea

➤ Both Florida men arrested this Spring in a scheme to launder funds for the fugitive "Gas King of Ukraine," through a Florida metals service center have entered guilty pleas.

John Can Unsalan, president of Orlando-based Metalhouse, LLC, and Sergey Karpushkin, a Belarusian citizen from Miami, and were indicted and arrested in April for engaging in a $150 million scheme to violate U.S. sanctions against Russian oligarch Sergey Kurchenko and his two companies. As set forth in court filings, between July 2018 and October 2021, Unsalan and Karpushkin conspired to transfer over $150 million to Kurchenko and sanctioned companies under Kurchenko's control.

The two engaged in trade with these sanctioned individuals and entities to procure steelmaking equipment and raw material despite knowing that they were prohibited doing business with them. They received tens of thousands of tons of metal products from the companies and agreed to share profits from these unlawful transactions. No licenses from OFAC were applied for or issued for these payments or transfers.

Unsalan pleaded guilty October 3 in U.S. District Court in Orlando, Fla., to one count of conspiracy to commit money laundering to promote violations of the IEEPA, which carries a maximum sentence of 20 years in prison. Unsalan also agreed to forfeit $160,416,948.56 in proceeds that he obtained as a result of the conspiracy.

On Sept. 13, co-conspirator Sergey Karpushkin pleaded guilty and agreed to forfeit over $4.7 million in criminal proceeds. Karpushkins plea acknowledged violation of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705; and other money laundering charges. Karpushkin and his company, Cogentra USA, received $4,723,625 in Proceeds from the Offense, which included generating false and misleading certificates for sanctioned goods expropriated from Russian-occupied Ukraine that would suggest that the goods, in fact, originated in Russia.

Kurchenko was sanctioned by OFAC in 2015 for his role in misappropriating Ukrainian state assets. His companies, Kompaniya Gaz-Alyans and ZAO Vneshtorgservis, were designated by OFAC in 2018 for providing material support to the separatist-controlled Donetsk People's Republic and Luhansk People's Republic in eastern Ukraine. [11211]

## Strategy on Countering Corruption Unveiled

➤ The recently unveiled United States Strategy on Countering Corruption by the Biden-Harris Administration delineates a systematic approach to address corruption through a series of well-defined measures. This initiative, detailed under five distinct pillars, seeks to enhance the efficiency and effectiveness of existing government frameworks, both within and outside U.S borders.

To curb corruption and its deleterious effects, the U.S. Government will organize its efforts around five mutually reinforcing pillars of work:

- Modernizing, coordinating, and resourcing U.S. Government efforts to fight corruption; ·
- Curbing illicit finance;
- Holding corrupt actors accountable;
- Preserving and strengthening the multilateral anti-corruption architecture; and,
- Improving diplomatic engagement and leveraging foreign assistance resources to advance policy goals. [11023]

*'For the first time, all 94 U.S. Attorneys' Offices have now adopted a single Voluntary Self-Disclosure policy.'*

**MARSHALL MILLER**

# Justice Official Talks National Security Compliance

In a recent speech, **Marshall Miller, principal associate deputy attorney general**, emphasized consistency, predictability, and transparency in the Department of Justice's (DOJ) approach to corporate enforcement, particularly in relation to national security.

Speaking at the Global Investigations Review in New York September 21, Mr. Miller spoke to themes central to DOJ's Corporate Enforcement, highlighting where enfocement is headed.

## Voluntary Self-Disclosure (VSD)

"If you've been following our message on corporate crime in the last year, I trust one thing has come through loud and clear: the Department is placing a new and enhanced premium on voluntary self-disclosure (VSD)."

Miller said that the DOJ emphasis on VSD, aims for a consistent approach across all its components. "For the first time, all 94 U.S. Attorneys' Offices have now adopted a single Voluntary Self-Disclosure policy," Miller said.

Companies that voluntarily disclose wrongdoings could receive more lenient treatment, exemplified by the case of **Corsa Coal Corporation**, whichearlier this year received a declination from the Criminal Division and the U.S. Attorney's Office for the Western District of Pennsylvania, despite having used bribes to secure $143 million in coal contracts from an Egyptian state-owned company through bribes paid by a third-party intermediary.

They received a declination from prosecution because they "stepped up and owned up."

## Mergers and Acquisitions

On the issues of mergers and acquisitions (M&A), Mr. Miller discussed how the DOJ is striving to avoid penalizing companies that acquire others with a history of misconduct, provided they engage in careful due diligence and remediation.

**Miller**

"The Criminal Division's Corporate Enforcement Policy also offers the incentive of the prospect of a declination — in essence, a safe harbor — for misconduct reported to the Department that is uncovered during pre- or post-acquisition due diligence."

The Criminal Division's Corporate Enforcement Policy also offers the incentive of the prospect of a declination — in essence, a safe harbor — for misconduct reported to the Department that is uncovered during pre- or post-acquisition due diligence.

"The Safran declination from December 2022 is a great example. There, the company voluntarily self-disclosed that two companies it acquired paid a consultant to win contracts with the Chinese government, knowing that some of the money would be used to bribe senior officials.

"The conduct ended prior to the acquisition, Safran timely voluntarily self-disclosed, cooperated, and remediated, and the company thus secured a declination with disgorgement."

## Penalties and Incentives

"It's important also to highlight the enormous gulf between the outcomes for companies that

**Continues on next page**

**Continued from previous page**

do the right thing — that step up and own up — and the consequences for companies that do the opposite."

Mr. Miller emphasized that companies not abiding by deferred prosecution agreements (DPAs) and non-prosecution agreements (NPAs) would face serious consequences, citing the case of Ericsson as a high-profile example where the company had to pay additional penalties for failing to honor its commitments under a DPA.

"Put simply, **Ericsson** failed to live up to its commitments. The company failed to timely disclose requested and highly relevant documents related to the bribery scheme at the time of resolution; and it failed to timely disclose additional evidence and allegations of other potential FCPA violations. And so it paid the price."

Earlier this year Justice rolled out a pilot program related to compensation systems, aimed at incentivizing good behavior within companies. "Every corporate resolution involving the Criminal Division will require that the resolving company include compliance-promoting criteria within its compensation and bonus system," he said.

### National Security Focus

The national security implications of corporate activities are central, according to Mr. Miller. He said companies are on the "front lines" of national security issues, such as sanctions, money laundering, and export control laws.

**The majority of corporate criminal resolutions since his return to the department have involved national security, with this number doubling from 2022 to 2023.** "The trend is real, it is accelerating, and at DOJ we're dedicating the resources necessary to counter the threat," Miller warned.

**"National security laws must rise to the top of your compliance risk chart**, with the recognition that even the most innocuous-looking transaction or activity could implicate our collective security." [11146]

---

FINCEN

# Gacki Spells Out Priorities

**NEWLY INSTALLED FINCEN DIRECTOR** *Andrea Gacki outlined her group's agenda including a whistleblower rewards program, rules targeting real estate and investment advisors, drug trafficking and the rollout of beneficial ownership information reporting requirements of the Corporate Transparency Act*

**Gacki**

*In a presentation to the Association of Certified Anti-Money Laundering Specialists October 3. Ms. Gacki walked attendees through her objectives since being named to head FinCEN in July. She served as chief of Treasury's Office of Foreign Assets Control (OFAC)*

*[Remarks edited for brevity*]

I have spent my first weeks at FinCEN getting to know the team better and getting up to speed on our work across the bureau. Even though I have worked closely with FinCEN for many years, I have still been surprised by the full scope of FinCEN's remit. From alerting consumers to fraudulent schemes, to working with financial institutions to ferret out sanctions and export control evasion schemes, to providing law enforcement agencies with critical financial intelligence — it is a wide range of critical work streams. And FinCEN is a small agency, particularly given the breadth of its mandate.

### Beneficial Ownership Information Implementation

FinCEN's efforts, in significant part, are focused on the implementation of the beneficial ownership information reporting requirements of the Corporate Transparency Act.

**First, why is the collection of beneficial ownership information important?** Illicit actors use opaque corporate structures to facilitate money laundering, corruption, sanctions and tax evasion, drug trafficking, fraud, and a host of other criminal offenses with impunity, while legitimate businesses and everyday Americans suffer from their misdeeds.

Simply put, implementing the Corporate Transparency Act will help untangle these opaque corporate structures, thereby allowing

enforcement authorities to go after criminals and protect our national security.

Through outreach events and educational materials, we are working hard to create a framework where most small businesses should be able to file their beneficial ownership information on their own.

Recently, we published our *Small Entity Compliance Guide*, which walks small businesses through the requirements in plain language. It is our hope that this guide serves as a primary resource for mom-and-pop shops, providing clarity on their reporting obligations and explanations on how to actually file their beneficial ownership information.

Our dedicated beneficial ownership information webpage also contains guidance documents, answers to frequently asked questions, introductory videos, quick reference guides, and other resources to ensure that reporting companies and the small business community have the tools they need to comply with the new requirements.

**And in just the past two weeks, we published:**

• *The Small Entity Compliance Guide* in eight additional languages (for a total of 11 languages.)

• An additional set of Frequently Asked Questions were added to our growing library. And we are working now to translate those Frequently Asked Questions into several languages.

• An introductory brochure, which can be printed, folded, and distributed to small businesses.

• And a Notice of Proposed Rulemaking that would extend the beneficial ownership information reporting deadline for certain reporting companies.

Ensuring that all parties understand the new beneficial ownership rules is a top priority for Treasury. We are working together with the business community to ensure that this nationwide registry is a success.

## FinCEN's Other Anti-Corruption Initiatives

While FinCEN is devoting significant resources to implementing the Corporate Transparency Act, our mandate is broad, and we also remain hard at work on other priorities, including other initiatives that support the Administration's strategy to counter corruption.

**The White House has identified combating corruption as one of its top priorities.** FinCEN, along with our Treasury colleagues, has been examining the money laundering risks and vulnerabilities with certain "gatekeeper" industries such as real estate and investment advisers, and identifying how best to address those risks.

### RESIDENTIAL REAL ESTATE

**In December 2021, FinCEN issued an Advance Notice of Proposed Rulemaking** to solicit public comment on a potential rule to address the vulnerability in the U.S. real estate market to money laundering and other illicit activity. We are currently developing a Notice of Proposed Rulemaking, the contours of which are still being determined. **FinCEN aims to issue this NPRM later this year.**

### INVESTMENT ADVISORS

**AML/CFT risks presented by investment advisers** is a priority for Treasury. As Treasury has noted on several occasions, investment advisers are not generally subject to comprehensive AML/CFT requirements under the Bank Secrecy Act (BSA). Along with our Treasury colleagues and other public and private stakeholders, we are assessing the AML/CFT risks this poses and identifying the best ways to mitigate those risks.

## Whistleblower Program

FinCEN also intends to issue a Notice of Proposed Rulemaking for FinCEN's newly established AML and sanctions whistleblower program.

Under the whistleblower program, FinCEN will be positioned to pay awards to eligible whistleblowers. While we work on the rulemaking necessary to fully implement this program, FinCEN is already receiving tips, investigating information received through those tips and making referrals to its enforcement colleagues at OFAC and the Department of Justice. [11214]

# Yellen: CFIUS Must be Targeted

**ACTIONS TO RESTRICT** foreign investment in the United States must be "carefully scoped and targeted," Treasury Secretary Janet Yellen said told attendees of the second annual Committee on Foreign Investment in the United States Conference. The inter-agency CFIUS reviews the national security implications of specific foreign investment in the U.S.

Yellen

"With CFIUS, close collaboration is complemented by smart policy," Ms. Yellen said in her remarks opening the conference. "Like other actions to protect our national security interests, CFIUS actions should be carefully scoped and targeted. And CFIUS must also reflect a changing world. As new threats and vulnerabilities emerge, our national security priorities shift in response, and CFIUS needs to evolve in parallel."

The Treasury Secretary stressed than an open investment climate is crucial, noting that in 2021, almost 8 million US workers were employed by majority-owned US affiliates of foreign multinational enterprises. That same year, affiliates contributed $1.2 trillion to US GDP.

"But national security is a foremost priority, and we deploy a wide range of tools to safeguard it," she said. "Certain investments by foreign persons in the US present national security risks. By rigorously reviewing these foreign investments, we safeguard our national security while keeping the US market an open and welcoming environment for investors. This preserves our status as the top recipient of foreign direct investment, which contributes to our economic strength."

Treasury Assistant Secretary for Investment Security **Paul Rosen** said CFIUS is putting a focus on enforcement of existing agreements. Up until this year, CFIUS had only issued two civil monetary penalties. But so far in 2023, two civil monetary penalties have been issued and several more are pending at various stages, he said. **"We are on track to have more civil monetary penalties issued this year than we have in our entire history.** This is on top of various warning letters and other actions that we have taken in response to violations of CFIUS regulations," he said.

Over the next year, Treasury will be issuing one or more notices of proposed rulemaking including updates to include measures that:

- Allow for increased efficiency and effectiveness in our case processing and review functions,
- Update the Committee's penalty and enforcement authorities,
- Sharpen and enhance the Committee's tools in the non-notified space, and
- Broadly ensure the Committee's tools and processes are best aligned to the current landscape, according to Mr. Rosen. [11092]

## Russian Elites, Proxies, and Oligarchs (REPO) Deputies Tackle Forfeitures

**DEPUTIES OF THE REPO TASK FORCE** met in Washington to enhance sanctions enforcement efforts and bolster ongoing oligarch asset forfeiture initiatives.

Participants from Australia, Canada, the European Commission, France, Germany, Japan, Italy, the United Kingdom, and the U.S. emphasized that those profiting from Russia's war "should not be able to be able to live lives of luxury," and that Task Force members will continue to identify and disrupt proxy networks that attempt to use global financial centers to store and access wealth. Deputies also discussed ongoing efforts to counter sanctions evasion and disrupt Russian efforts to acquire critical dual-use technologies that fuel the Russian war machine.

Following the G7 Leaders commitment in May, the REPO Task Force has completed its initial effort to map and account for Russian sovereign assets that are immobilized and held in member jurisdictions. The total value of assets in this mapping exercise is estimated at around $280 billion, the majority of which is held in the EU.

The U.S. and the EU are examining ways to either seize Russian assets permanently or invest them and use the windfall proceeds to help rebuild Ukraine. In December, Congress authorized the Justice Department to transfer assets seized from sanctioned Russian oligarchs to the State Department for Ukrainian reconstruction. But the power applies only to assets confiscated in connection with violating U.S. sanctions under certain presidential executive orders. [11030]

# CHIPS Act Security Rule Released

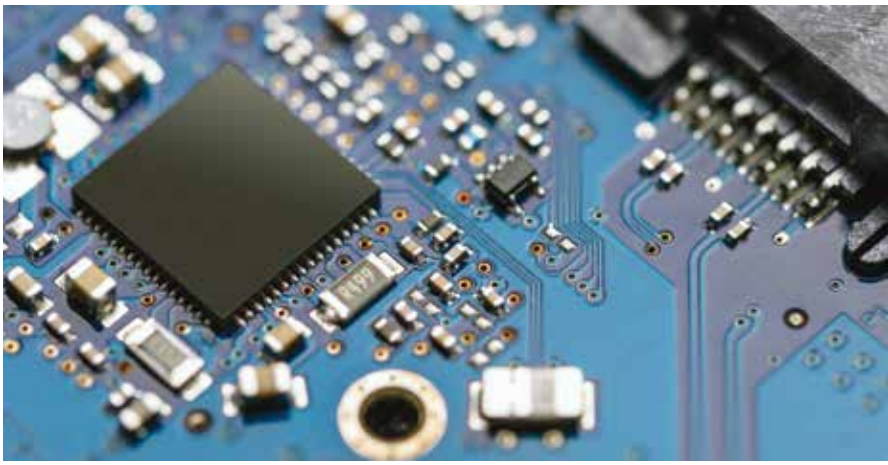
The U.S. Department of Commerce recently released the final rule implementing the national security guardrails of the bipartisan CHIPS and Science Act.

The rule elaborates on two core provisions of the statute: first, prohibiting CHIPS funds recipients from expanding material semiconductor manufacturing capacity in foreign countries of concern for ten years; and second, restricting recipients from certain joint research or technology licensing efforts with foreign entities of concern.

The rule will help ensure CHIPS investments enhance global supply chain resilience in coordination with allies and partners. The CHIPS and Science Act is part of President Biden's Investing in America agenda for unleashing a manufacturing and innovation boom, driving U.S. competitiveness, and strengthening economic and national security.

This final rule follows consideration of comments submitted in response to the proposed rule published in March 2023. The Department reviewed and incorporated suggestions from stakeholders, including representatives of the domestic and foreign semiconductor industry, academia, labor organizations, trade associations and others in developing this rule. The rule offers details and definitions on national security measures applicable to the CHIPS Incentives Program, including limiting funding recipients from expanding semiconductor manufacturing in foreign countries of concern.

"One of the Biden-Harris Administration's top priorities — made possible by the CHIPS and Science Act — is to expand the technological leadership of the U.S. and our allies and partners. These guardrails will protect our national security and help the United States stay ahead for decades to come," said **Secretary of Commerce Gina Raimondo**.



**The CHIPS and Science Act classifies semiconductors as Critical to National Security.**

ADOBE STOCK / GRAFVISION

"CHIPS for America is fundamentally a national security initiative and these guardrails will help ensure companies receiving U.S. Government funds do not undermine our national security as we continue to coordinate with our allies and partners to strengthen global supply chains and enhance our collective security."

The statute:

• Prohibits recipients of CHIPS incentives funds from using the funds to construct, modify, or improve a semiconductor facility outside of the U.S.;

• Restricts recipients of CHIPS incentives funds from investing in most semiconductor manufacturing in foreign countries of concern for 10 years after the date of award; and,

• Limits recipients of CHIPS incentives funds from engaging in certain joint research or technology licensing efforts with a foreign entity of concern that relates to a technology or product that raises national security concerns.

• If these guardrails are violated, the Department can claw back the entire federal financial assistance award.

The final rule provides details on and defini-

**Continues on next page**

**Continued from previous page**

tions for these national security guardrails. In particular, the rule:

• **Establishes Standards to Restrict Expansion of Advanced Facilities in Foreign Countries of Concern.** The statute prohibits the material expansion of semiconductor manufacturing capacity for leading-edge and advanced facilities in foreign countries of concern for 10 years from the date of award. In addition to front-end and back-end processes, the rule clarifies that wafer production is included within the definition of semiconductor manufacturing. The final rule ties expanded semiconductor manufacturing capacity to the addition of cleanroom or other physical space and defines material expansion as increasing a facility's production capacity by more than five percent. This threshold is intended to capture even modest transactions to expand manufacturing capacity but allows funding recipients to maintain their existing facilities through normal course-of-business equipment upgrades and efficiency improvements.

• **Limits the Expansion of Legacy Facilities in Foreign Countries of Concern.** The statute places limits on the expansion and new construction of legacy facilities in foreign countries of concern. The rule provides details regarding this restriction, prohibiting recipients from adding new cleanroom space or production lines that result in expanding a facility's production capacity beyond 10 percent. The rule establishes a notification process for recipients that have plans to expand legacy chip facilities so the Department can confirm compliance with the national security guardrails.

• **Classifies Semiconductors as Critical to National Security.** While the statute allows companies to expand production of legacy chips in foreign countries of concern in limited circumstances, today's rule classifies a list of semiconductors as critical to national security, thereby subjecting them to tighter restrictions. This designation covers chips that have unique properties critical to U.S. national security needs, including chips used for quantum computing, in radiation-intensive environments, and for other specialized military capabilities. This list of semiconductor chips was developed in consultation with the Department of Defense and U.S. Intelligence Community.

• **Details Restrictions on Joint Research and Technology Licensing Efforts with Foreign Entities of Concern.** The statute restricts covered entities from engaging in joint research or technology licensing with a foreign entity of concern that relates to a technology or product that raises national security concerns. Foreign entities of concern include those owned or controlled by foreign countries of concern, those on the Bureau of Industry and Security (BIS) Entity List and Treasury Department's Chinese Military-Industrial Complex Companies (NS-CMIC) list, and others as outlined in the statute. This restriction does not apply to several types of engagements which are necessary to existing operations and do not threaten national security, such as activities related to international standards, involving patent licensing, and to enable funding recipients to utilize foundry and packaging services.

## International Coordination with U.S Partners and Allies

The Department will continue coordinating with allies and partners, including through engagements with the Republic of Korea, Japan, India, and the UK, and through the Indo-Pacific Economic Framework, European Union-United States Trade and Technology Council, and North American Semiconductor Conference.

This coordination is in support of a healthy global semiconductor ecosystem that drives innovation and is resilient to cybersecurity threats, natural disasters, pandemics, geopolitical conflict, and more. [11149]

# BRIEF

## Small Businesses Report Beneficial Ownership Compliance Guide

➤ Financial Crimes Enforcement Network (FinCEN) published a Small Entity Compliance Guide to assist the small business community in complying with the beneficial ownership information (BOI) reporting rule.

Foreign companies that register in U.S. states after Jan. 1 may need to report beneficial ownership information to comply with the Corporate Transparency Act.

Starting in 2024, many entities created in, or registered to do business in, the United States will be required to report to FinCEN information about their beneficial owners — the individuals who ultimately own or control a company.

The Guide is intended to help businesses learn about and comply with the new reporting requirements.

FinCEN is also issuing revised and new FAQs about the BOI reporting requirements that incorporate content from the Guide. Additional translated versions of the Guide and the FAQs will be posted to FinCEN's website soon. [11109]

# Treasury Ratchets up Russian Sanctions

**THE OFFICE OF FOREIGN ASSETS CONTROL** (OFAC) continues to target Russian elites and firms that benefit from their affiliations with Russia's defense sector, military-industrial complex, and the Kremlin. On September 13, OFAC imposed nearly 100 sanctions on Russian elites, Russia's industrial base, financial institutions, and technology suppliers. Additionally, they made designations of more than 70 individuals.

Industries affected include Railroad Equipment, heavy machinery, digital optical systems, diamond traders, and advisors of the Wagner Group to the president of the Central African Republic.

On May 19, 2023, G7 Leaders pledged to focus on those operating in Russia's manufacturing and construction sectors. Reinforcing that commitment, OFAC sanctioned several leading Russian manufacturing and construction firms.

Additional sanction categories included:

• Further Limiting Russia's Revenue from Extractives and Future Extractives Capabilities

• Curtailing Russia's Access to the International Financial System

• Several Russia-based wealth management, consulting, auditing, and investment firms have been designated. [11079]


**Kirov Works, St. Petersburg**

# OFAC Names Finns & Turks in Russian Action

**ALONG WITH NUMEROUS** Russian entities and persons, OFAC hasdesignating a Finland-based network that specializes in shipping foreign electronics to Russia-based end-users, as well as Turkish firms involved in the shipment of dual-use items into Russia.

## Finland: Siberica and Luminor Network

OFAC is designating a Finland-based network that specializes in shipping foreign electronics to Russia-based end-users. Finland-based logistics firms **Siberica Oy** (Siberica) and **Luminor Oy** (Luminor) have sent a wide variety of electronics into Russia, including UAV cameras, high-performance optical filters, and lithium batteries. French national Gabriel Temin is Siberica's owner, managing director, and a member of Siberica's board of directors and Estonian national **Catherine Esther Temin** is a deputy board member of Siberica.

## Türkiye-based Companies

Russia continues to rely on third-country entities to keep importing much-needed dual-use goods to enable its unprovoked war of aggression on Ukraine. The U.S. Department of the Treasury has repeatedly raised the issue of the shipment or transshipment of dual-use goods to Russia with the Government of Türkiye and the Turkish private sector. Today, OFAC is targeting two entities based in Türkiye.

**Margiana Insaat Dis Ticaret Limited Sirketi** (Margiana) has made hundreds of shipments to Russia-based entities Limited Liability Company SMT-iLogic (SMT-iLogic) and Saturn EK OOO (Saturn EK), which were designated pursuant to E.O. 14024 on May 19, 2023 and July 20, 2023, respectively. SMT-iLogic is known to be involved in the supply chain for producing Russian military UAVs used in Russia's war against Ukraine. Margiana's shipments to SMT-iLogic and Saturn EK have included High Priority Items of the kind recovered in multiple Russian weapons systems used against Ukraine, including the Kalibr cruise missile, the Kh-101 cruise missile, and the Orlan-10 UAV.

**Demirci Bilisim Ticaret Sanayi Limited Sirketi** (Demirci), founded in March 2022, has sent sensors and measuring tools into Russia. [11080]

# BRIEFS

## Sudan: Further Sanctions, Oil Firm Execs Finally Face Trial

➤ Treasury's Office of Foreign Assets Control (OFAC) sanctioned a Sudanese Military Leader for his command of an entity whose members have engaged in acts of violence and human rights abuses, including the massacre of civilians, ethnic killings, and use of sexual violence. Abdelrahim Hamdan Dagalo led the Rapid Support Forces in the Darfur region.


Meanwhile, in Stockholm, trial has begun for two senior executives of Lundin Oil, responsible for engaging the Sudanese Armed Forces to ensure security for their production interests in South Sudan in between 1997 and 2003.

Ian Lundin, the son of the firm's founder, and former CEO Alex Schneiter, stand accused of endorsing aerial bombings, killing of civilians and burning of entire villages, according to the prosecution. Other partners in the venture were Malaysia's Petronas Carigali Overseas, OMV (Sudan) Exploration GmbH of Austria, and the Sudanese state-owned oil company Sudapet Ltd.

Lundin Energy was purchased by Aker BP in July 2022 in a deal worth more than US$14 billion. At the time, the firm's largest shareholders included Black Rock, Vanguard and T. Rowe Price. [11021]

## Treasury Sanctions Iran Facilitators

➤ The Treasury Department announced it has imposed sanctions on seven individuals and four entities based in Iran, the People's Republic of China, Russia and Türkiye in connection with Iran's unmanned aerial vehicle and military aircraft development.

This network has facilitated shipments and financial transactions in support of the US-designated Iran Aircraft Manufacturing Industrial Company's (HESA's) UAV and military aircraft production, procurement and maintenance activities.

HESA manufactures Iran's Ababil- and Shahed-series UAVs. HESA has been using the name Shahin Company in contracts with overseas-based suppliers in an apparent effort to evade US sanctions and export controls. Because HESA continues to procure sensitive UAV components under this name, HESA's entry on the SDN List is being updated to include Shahin Company as an alias.

PRC-based Shenzhen Jiasibo Technology Company Limited is operated by US-designated HESA supplier Yun Xia Yuan. Yun has used Shenzhen Jiasibo, in conjunction with her other U.S.-designated firms, S&C Trade PTY Company Limited and Shenzhen Caspro Technology Company Limited, to facilitate the supply of aerospace-grade radar altimeter systems, GPS and VHF antennas, sensors and other hardware with possible UAV applications to HESA.

Russia-based Delta-Aero Technical Service Center LLC is being sanctioned for supplying propellers and tires to HESA for its AN-140 aircraft, which HESA has outfitted for military use. Russia-based Joint Stock Company Scientific Production Enterprise Aerosila has performed ground and flight tests for HESA and facilitated the supply of auxiliary power units for the Iran-based firm. Russia-based Joint Stock Company Star has contracts with HESA to overhaul components of HESA's AN-140 aircraft.
[11131]

## Iran: Qatar Aid Channel, and further sanctions

➤ The U.S. government announced the establishment of a humanitarian channel in Qatar (HC) to further facilitate the flow of humanitarian assistance to the people of Iran consistent with the U.S. government's longstanding support for humanitarian trade. Similar to humanitarian channels established under previous administrations, the HC is designed to support the Iranian people's access to food, agricultural goods, medicine, and medical devices under stringent due diligence measures that guard against money laundering, misuse, and evasion of U.S. sanctions. The HC does not lift any U.S. sanctions on Iran, and the U.S. government continues to impose sanctions on Iran's malign activity, including in response to Iran's weapons proliferation and its support for international terrorism.

Concurrently, Treasury's Office of Foreign Assets Control (OFAC) designated Mahmoud Ahmadinejad, the former president of Iran, for having provided material support to the Iranian Ministry

of Intelligence and Security (MOIS), an entity re-designated by the Department of State.

During Ahmadinejad's term in office, MOIS was involved in the detention of several U.S. nationals, including former Federal Bureau of Investigations (FBI) special agent Robert "Bob" Levinson, as well as three U.S. hikers: Shane Bauer, Joshua Fattal, and Sarah Shourd. While the three hikers were eventually released after years-long detentions, Mr. Levinson remains missing and is presumed deceased.[11110]

## OFAC: Issuance of Russia-related General Licenses

➤ **Japanese Imports of Siberian Oil & Gas**

Treasury's Office of Foreign Assets Control (OFAC) is issuing Russia-related General License 55A, "Authorizing Certain Services Related to Sakhalin-2": Maritime transport of crude oil originating from the Sakhalin-2 project ("Sakhalin-2 byproduct") is authorized through 12:01 a.m. eastern daylight time, June 28, 2024, provided that the Sakhalin-2 byproduct is solely for importation into Japan.

➤ **Russia Wind Down Transactions**

Russia-related General License 72, "Authorizing the Wind Down of Transactions Involving Certain Entities Blocked on September 14, 2023." Ordinarily incident and necessary to the wind down of any transaction involving one or more of eight blocked persons (collectively, the "Blocked Entities") are authorized through December 13, 2023, provided that any payment to a Blocked Entity is made into a blocked account in accordance with the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587 (RuHSR): Russian Copper Company; United Metallurgical Company; Transmashholding JSC; JSC Avtovaz; Moscow Automotive Factory Moskvich; Machine Building Plant Tonar; Publichnoe Aktsionernoe Obschestvo Sollers; Arctic Transshipment Limited Liability Company; or any entity in which one or more of the above persons own, directly or indirectly, individually or in the aggregate, a 50 percent or greater interest. [11078]


**Tonar is the leading Russian Trailer Manufacturer**

**Doha, Qatar.**
ADOBE STOCK

## State: New Sanctions To Protect Ukraine's Children

➤ "On Ukrainian Independence Day, we are sanctioning two entities and 11 individuals for their involvement in the forcible transfer of Ukraine's children to Russia-occupied areas. Ukraine's children are not forgotten," said Secretary Blinken on Twitter.

The Department of State is imposing sanctions and pursuing visa restrictions on individuals and entities connected to forcible transfer and deportation of Ukraine's children.

Some targets are being designated pursuant to Executive Order (E.O.) 14024 , which authorizes sanctions with respect to specified harmful foreign activities of the Government of the Russian Federation, while others are subject to a visa restriction policy under Section 212(a)(3)(C) of the Immigration and Nationality Act, which authorizes the Secretary of State to restrict visa issuance to Russian Federation military officials and Russia-backed or Russia-installed purported authorities who have been involved in human rights abuses, violations of international humanitarian law, or public corruption in Ukraine.

Find details in the fact sheet "Imposing Sanctions and Visa Restrictions on Individuals and Entities to Promote Accountability for Forced Transfer and Deportation of Children During Russia's Illegal War Against Ukraine." [10989]

**To read the complete stories, click on the blue codes, or search for that number at www.exportprac.com**