WorldECR

ISSUE 76. FEBRUARY 2019
www.WorldECR.com

Rusal et al taken off the SDN list

On 27 January, the US Treasury announced in a (by its standards, terse) press release that, following a notification submitted to Congress on 19 December, OFAC had 'lifted sanctions imposed on En+ Group plc ("En+"), UC Rusal plc ("Rusal"), and JSC EuroSibEnergo ("ESE").'

In its release, the Treasury said: 'Under the terms of their removal from OFAC's [SDN list], En+, Rusal, and ESE have reduced Oleg Deripaska's direct and indirect shareholding stake in these companies and severed his control.

'This action ensures that the majority of directors on the En+ and Rusal boards will be independent directors – including U.S. and European persons – who have no business, professional, or family ties to Deripaska or any other SDN, and that independent U.S. persons vote a significant bloc of the shares of En+.'

It added that the companies had also agreed to 'unprecedented transparency for Treasury into their operations by undertaking extensive, ongoing auditing, certification, and reporting requirements,' while the sanctions imposed on Oleg Deripaska continue to be in force.

'Under the terms of their removal from OFAC's [SDN list], En+, Rusal, and ESE have reduced Oleg Deripaska's direct and indirect shareholding.'

Douglas Jacobson, of DC firm Jacobson Burton Kelley PLLC, told *WorldECR*, this was 'the right decision,' despite the 'knee-jerk reaction' of some lawmakers.

'[T]his delisting was long overdue,' he said, 'and will be of great relief to many US companies that purchase and sell to Rusal and the other two parties removed from the SDN List yesterday. Despite the knee-jerk reaction from some members in Congress, this decision was the correct one and shows that US sanctions, when used properly, can effect real change and the person who was targeted, Mr. Deripaska, will not benefit from the delisting.'

> ***'Despite the knee-jerk reaction from some members in Congress, this decision was the correct one.'***
>
> **Douglas Jacobson**

In Jacobson's view, 'OFAC and Treasury's TFI are professionally run organisations and recognise the need to balance sanctions and legitimate business. While the US Congress certainly has a right to oversee OFAC, these types of decisions are not taken lightly and there is no need for Congress to second-guess these determinations.'

When the sanctions were imposed in April 2018, they were described by one observer as 'far and away the most significant sanctions action...since the imposition of sectoral sanctions in 2015.'

A supply chain assessment prepared by the Atlantic Council last May found that the immediate impact of the designation of Rusal included: a 33% spike in the price of aluminium, a 50% drop in Rusal's share price, and termination of deliveries of bauxite to Rusal refineries by Rio Tinto and of shipments by Maersk. The designation had an impact on many tens of thousands of people.

EN+ has said Deripaska's interest in the company has been reduced 'to no more than 44.95%' in part achieved by VTB Bank 'taking ownership of certain of shares pledged as collateral for previously issued obligations of entities controlled by Mr Deripaska issued by VTB Bank; the bank has no voting rights with respect to those shares with the rights held by an independent American voting trustee' and the donation by Oleg Deripaska 'of certain shares to a charitable foundation.'

Lord Barker of Battle, the company's independent chairman said: 'The lifting of sanctions on the whole En+ Group is a turning point in this great company's fortunes. This is the first time independent directors of a London listed Russian company, with the strong support of minority shareholders, have successfully removed control from a majority shareholder as a direct response to US sanctions policy. It is a clear victory for muscular corporate governance and sets the group on a new path as an independent, international leader in its sector, operating in 14 countries across five continents.'

OFAC acts against Iran-backed militias

On 24 January OFAC said it had taken action against:

- The Fatemiyoun Division and Zaynabiyoun Brigade (two Syria-based, Iran-backed militias composed of foreign nationals)
- Qeshm Fars Air, an Iranian airline linked to designated Iranian airline Mahan Air and Iran's Islamic Revolutionary Guard Corps-Qods Force, and
- Flight Travel LLC, an Armenian general sales agent (GSA) providing services to Mahan Air.

'The brutal Iranian regime exploits refugee communities in Iran, deprives them of access to basic services such as education, and uses them as human shields for the Syrian conflict. Treasury's targeting of Iran-backed militias and other foreign proxies is part of our ongoing pressure campaign to shut down the illicit networks the regime uses to export terrorism and unrest across the globe,' said Treasury Secretary Steven Mnuchin.

See: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190124.aspx

Consultation closes. Pandora's box opens

Time is up for submitting responses to the US Commerce Department's consultation on new controls on emerging technologies. Debate about what's appropriate, the consequences of new controls, and how to apply them is likely to continue long after.

The advance notice of proposed rulemaking ('ANPRM'), published 14 November, sought 'public comment on criteria for identifying emerging technologies that are essential to U.S. national security, for example because they have potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or intelligence advantage.' It is intended as a response – at least in part – to the 'Made in China 2025' initiative and its emphasis on encouraging indigenous production of emerging tech sectors including artificial intelligence, robotics and quantum mechanics.

Proposed controls on new technologies such as AI are causing controversy in the US and abroad.

National security aims

The US consultation lists 14 technologies for which it 'seeks to determine whether there are specific emerging technologies that are essential to the national security of the United States,' amongst them biotechnology, AI, position navigation and timing technology ('PNT'), brain computer interfaces, quantum computing, additive manufacturing and robotics.

By the time that the BIS consultation had closed (10 January – the deadline had been extended by public demand) it had received 238 submissions. Typically, the Commerce Department would perform a preliminary review of the comments and then post them for public inspection; however, due to the US government shut-down, comments are not yet publicly available (save three posted before the shut-down in December).

Draft comments circulated privately for review indicate some industries and their advisers are concerned about likely unintended consequences and the impact of new controls on a broad sweep of companies using state-of-the-art technology in everyday products.

Melissa Duffy, partner at the Washington DC office of law firm Dechert, told *WorldECR* that she understood the prospect of new controls on AI has concerned numerous companies and trade associations: 'It's getting people excited because it potentially touches on more industries than some of the other emerging technologies on the list. It's an area where you will struggle to make some key distinctions between military and civilian capabilities. While some of its applications are very relevant to the military, many of the greatest advancements are being made in the civilian sector – such as autonomous vehicles, where the use of AI is essential, and human safety is on the line.'

And, she says, it would be difficult to control according to the kinds of technical thresholds used to distinguish between military or civilian applications of other technologies – such as sensors, ubiquitous in everyday applications but in some cases subject to different levels of control according to specific characteristics (such as those relevant to missiles, rockets or other military end uses).

'Broader commercial implications are not only that unilateral controls could disadvantage US companies, but that R&D, much of which is conducted in partnership with overseas companies or subsidiaries, and the ability to generate global economies of scale would both be affected.'

Through 3D glasses

Another technology in the purview of the ANPR is additive manufacturing, or so-called '3D Printing', the threat of which, says Dr Grant Christopher, director of nonproliferation at London-based Ridgeway Information, is generally poorly understood.

There are, points out Christopher, several kinds of AM technology – ranging from the machines popular with hobbyists (limited in capability, to moulding in plastic and unlikely to be put to use, for example, in a nuclear fuel cycle, nuclear weapon or missile delivery system, though it may stretch to a handgun), to 'very interesting' and vastly more sophisticated technology using powder metallurgy. These use lasers to melt powdered aluminium, nickel or maraging steel, which is then rapidly cooled.

But, he says, while the latter possess huge potential, not only are they proportionately expensive, but using them requires skills and training that are difficult to acquire outside of the best-resourced institutes or R&D centres.

'It is an extremely complex process, and the physics gets complicated very quickly,' says Christopher. 'The Universal Replicator on Star Trek it isn't! … I know that [a major corporation] which is using these machines finds that it can take months to initially commission the machines, each one of which has to be fine-tuned to perform as required. It is difficult to print the same part twice in a row. Post-processing is difficult and necessary, and demands the use of CT scanners…'

In short, he says, most proliferators, rogue states or non-state actors would find it easier and cheaper to acquire controlled parts by other means than through additive manufacturing. It is also not clear if additive manufacturing today can substitute for any existing conventional processes.

continues over

Fit for purpose?
Aside from the technical elements of the consultation, it also begs the question as to whether the underlying rationale for the ANPR is the same as that for export controls as typically understood. This is a point raised by Japan's Center for Information on Security Trade Control ('CISTEC') in its submission, observing that under the Export Control Reform Act ss.1758 (a) and (b) technologies essential to the national security of the US should be identified as 'Emerging' and 'Foundational', and that their export and re-export should be subject to licence requirements.

Section 1758 (c) stipulates that the US government would propose that any so-identified technologies be added to the multilateral export control regime control lists.

'However,' (the CISTEC submission notes), 'it is difficult for us to understand the substantial relationships between [sections (a), (b), and (c)] for the following reasons: international export control regimes aim to prevent the transfer or diversion of high-tech products and technologies to countries of concern related to weapons of mass destruction and conventional weapons and terrorists in order to ensure international peace and security, and they are not intended for national security of a specific country.' Perhaps another consultation is due?

A similar ANPR for 'foundational technologies' is planned for later this year.

Links and notes
The consultation and responses are at:
https://www.regulations.gov/docket?D=BIS-2018-0024

Transfer PdVSA control to Guaido: Mnuchin

'The United States is ramping up its action against the Venezuelan government. On 28 January, the Department of the Treasury's Office of Foreign Assets Control ('OFAC') said it had designated PdVSA, Venezuela's state oil company, 'pursuant to Executive Order (E.O.) 13850 for operating in the oil sector of the Venezuelan economy.'

Treasury Secretary, Steven Mnuchin said: 'The United States is holding accountable those responsible for Venezuela's tragic decline and will continue to use the full suite of its diplomatic and economic tools to support Interim President Juan Guaidó, the National Assembly, and the Venezuelan people's efforts to restore their democracy.'

He said that the designation would 'help prevent further diverting of Venezuela's assets by [President] Maduro and preserve these assets for the people of Venezuela,' and described 'the path to sanctions relief for PdVSA' as being through the 'expeditious transfer of control to the Interim President or a subsequent, democratically elected government.'

On 26 January, EU High Representative Federica Mogherini said that the EU 'reiterates its full support to the National Assembly, which is the democratic legitimate body of Venezuela, and whose powers need to be restored and respected, including the prerogatives and safety of its members.' She called for the holding of free, transparent and credible presidential elections 'in accordance with internationally democratic standards and the Venezuelan constitutional order.'

Mogherini said that in the absence of an announcement on the organisation of fresh elections with the necessary guarantees, the EU 'will take further actions, including on the issue of recognition of the country's leadership in line with article 233 of the Venezuelan constitution.' This has been interpreted as a message of support for Guaidó.

OFAC is amending a number of extant licences relating to dealings with Venezuela.

Links and notes
https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190128.aspx

A new year, a new home

2019 sees a number of moves within the trade compliance community. **Diego Pol** has joined law firm Dentons' Barcelona office as a partner. He joins from Baker McKenzie and will head his new firm's Spanish compliance practice. Meanwhile, also at Dentons, the Brussels office has hired senior associate **Nicoleta Tuominen** from Freshfields and has opened an office in Düsseldorf, which will be headed by new office managing partner **Andreas Haak**, who joins from Taylor Wessing and is accompanied by his colleague **Dr Barbara Thiemann**.

In Washington DC, **Barbara Linney**, formerly member at law firm Miller & Chevalier, joins the DC office of Baker Hostetler, while **Ginger Faulk** left Baker Botts at the end of 2018 to join the DC office of Eversheds Sutherland.

On other side of the country, **Steven Brotherton** has joined KPMG US as Principal, Global Export Control & Sanctions lead, working out of its San Francisco office. Steve joins from STR Trade.

European unity
Of particular note this month is the creation of **AT-ICA**, a 'European association of trade and investment controls and compliance attorneys.' The association, whose members feature regular contributors to *WorldECR*, brings together a host of firms from Europe and the Middle East, including, but not limited to, Herzog Fox & Neeman, Studio Legale Padovan, Kromann Reumert, Mannheimer Swartling, Loyens & Loeff, Addleshaw Goddard, Thommessen and others. Key areas of practice for members include sanctions and export controls, anti-bribery and corruption and foreign direct investment issues.

See: https://www.at-ica.com/

‘Deep political intentions behind Huawei charges,’ says China

The US Justice Department has charged the Chinese telecom company Huawei, two of its affiliates (Huawei USA and Skycom), and its chief financial officer Meng Wanzhou with a number of offences, including financial fraud, money laundering offences, conspiracy to defraud the United States, and sanctions violations.

China has accused the United States of ‘bashing on’ Chinese companies, and said ‘deep political intentions’ lie behind the charges, which were announced by senior ‘officials from the US Department of Justice, the Federal Bureau of Investigation, the US Department of Commerce, and the Department of Homeland Security.’

United States Attorney Richard Donoghue said: ‘As charged in the indictment, Huawei and its subsidiaries, with the direct and personal involvement of their executives, engaged in serious fraudulent conduct, including conspiracy, bank fraud, wire fraud, sanctions violations, money laundering and the orchestrated obstruction of justice. For over a decade, Huawei employed a strategy of lies and deceit to conduct and grow its business. This Office will continue to hold accountable companies and their executives, whether here or abroad, that commit fraud against U.S. financial institutions and their international counterparts and violate U.S. laws designed to maintain our national security.’

Fair treatment

Reacting to the charges, China’s foreign ministry spokesman Geng Shuang said that the Chinese government has ‘all along urged Chinese companies to conduct international economic cooperation on the basis of complying with relevant laws and regulations,’ but at the same time, China asked ‘that all countries provide a fair, just and non-discriminatory environment for the normal operations of Chinese companies.’

Geng said, ‘For some time, the US has been using national power to tarnish and crack down on specific Chinese companies in an attempt to strangle their lawful and legitimate operations. Behind such practices are deep political intentions and manipulations. We strongly urge the US to stop its unreasonable bashing on Chinese companies including Huawei, and treat them objectively and fairly. China will also continue to uphold the lawful and legitimate rights and interests of Chinese companies.’

Commenting on the predicament of Ms Meng, Geng said that the United States had ‘abused’ their bilateral agreement, violating the rights and interests of a Chinese citizen.

‘Once again we urge the US to immediately withdraw its arrest warrant for Ms. Meng Wanzhou, refrain from making a formal extradition request, and stop going further down the wrong path. We also urge Canada to take China's solemn position seriously, immediately release Ms. Meng Wanzhou and ensure her lawful and legitimate rights and interests and stop risking its own interests for the benefits of the US.’

According to one Washington DC lawyer, the US government’s pursuit of Huawei threatens to have huge implications for global supply chains in the telecommunications sector.

Links and notes

The indictment, redacted in parts, is at:
https://www.justice.gov/opa/press-release/file/1125021/download

EU imposes first chemical weapons sanctions

On 21 January, the Council of the EU imposed sanctions for the first time on entities and persons under its new regime of restrictive measures against the use and proliferation of chemical weapons. Among the designations are those of individuals believed responsible for the poisoning of members of the Skripal family in Salisbury, England. Those individuals have already been designated by the US Office of Foreign Assets Control (‘OFAC’).

The Council said: ‘[T]he designations include the two GRU officials, and the Head and Deputy Head of the GRU (also known as the G.U., or the Main Directorate of the General Staff of the Russian Armed Forces) responsible for possession, transport and use in Salisbury (UK) of a toxic nerve agent on the weekend of 4 March 2018.

‘Sanctions are also imposed on the Syrian entity responsible for the development and production of chemical weapons, the Scientific Studies and Research Centre (SSRC), as well as five Syrian officials directly involved in the SSRC’s activities.’ It says that the designations, which impose a travel ban and asset freeze, contribute ‘to the EU's efforts to counter the proliferation and use of chemical weapons which poses a serious threat to international security.’

Links and notes

The Council Decision is at: https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:32019D0086&from=enSee also:https://www.consilium.europa.eu/en/press/press-releases/2019/01/21/chemical-weapons-the-eu-places-nine-persons-and-one-entity-under-new-sanctions-regime/pdf

Germany blocks Mahan Air

Germany has banned Iran's Mahan Air from landing in the country. A spokesperson for Chancellor Angela Merkel told reporters that it could not be 'ruled out that this airline carries out transports to Germany that affect our security concerns. This is especially true against the backdrop of terrorist activities, intelligence on terrorist activities from the Iranian side and Iranian entities in Europe in the past.'

Iran's Civil Aviation Organization: decision to suspend the company's operating licence is 'unjustifiable and not professional',

Mahan Air was designated by the United States in 2011 'for providing financial, material and technological support to the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF).'

It is known that the US ambassador to Germany, Richard Grenell, has assiduously lobbied the German government to ban Mahan Air, and the decision has been warmly welcomed by US Secretary of State Mike Pompeo.

Iran's Civil Aviation Organization has described the decision to suspend the company's operating licence as 'unjustifiable and not professional', according to the Islamic Republic News Agency, IRNA.

It said: 'Mahan has had all the necessary licences. The suspension is in line with the economic war that's been waged against the Iranian nation. Iran's civil aviation has always been exposed to limitations caused by the animosity of ill-wishers and its foreign rivals.'

Grand Duchy publishes export control law

On 14 December 2018, Luxembourg's new export control law and regulation were published in the Grand Duchy's Official journal – implementing the law of 27 June 2018.

'The Law of 27 June 2018' concerns:

- 'the control of the export, transfer, transit and importation of goods of a strictly civil nature, defence-related products and dual-use goods;
- brokerage and technical assistance;
- the intangible transfer of technology;
- the implementation of United Nations Security Council resolutions and acts adopted by the European Union containing trade restrictive measures against certain States, political regimes, persons, entities and groups and repealing:
  - the amended law of 5 August 1963 concerning the import, export and transit of goods;
  - the Act of 5 August 1963 concerning the surveillance of imports, exports and the transit of goods;
  - the law of 28 June 2012 on the conditions for transfers of defence-related products in the European Union.'

Links and notes

See the new regulations at:
http://legilux.public.lu/eli/etat/leg/loi/2018/06/27/a603/jo
http://legilux.public.lu/eli/etat/leg/rgd/2018/12/14/a1158/jo

Pakistan updates control list

In December, Pakistan's Strategic Export Control Division ('SECDIV') announced that 'pursuant to the Export Control on Goods, Technologies, Material and Equipment related to Nuclear and Biological Weapons and their Delivery Systems Act 2004, the Government of Pakistan has notified revised Control Lists of Goods, Technologies, Material and Equipment that are subject to SECDIV license for export. The Act enables the Government to control export, re-export, transshipment and transit of goods, technologies, material and equipment related to Nuclear and Biological Weapons and their Delivery Systems.'

It said that, '[T]he revised Control Lists have been notified vide Gazette of Pakistan S.R.O. 891(I)/2018 dated 5 July 2018. It may be mentioned that the lists were originally notified in 2005 and subsequently revised in 2011, 2015 and 2016.'

International alignment

SECDIV notes that the control lists 'are harmonized with the standards and lists of international export control regimes i.e. the Nuclear Suppliers Group, the Missile Technology Control Regimes [sic] and the Australia Group and incorporate the latest changes/updates made by these export control regimes. The notification signifies the continuing resolve and policy of Pakistan as a responsible nuclear state to advance the shared goals of non-proliferation and strictly adhere to its commitments.'

Never-ending Brexit uncertainty raises further export and sanctions questions

The crushing defeat of UK Prime Minister Theresa May's withdrawal agreement in the House of Commons brings the prospect of a 'no-deal' Brexit on 30 March closer, with implications for exporters.

In December, the European Union enacted a package of 'bare bones' emergency measures aimed at mitigating disruption in financial services, air transport, climate policy, and customs.

These include a proposed amendment to EU Council Regulation (EC) No 428/2009 ('the Dual-Use Regulation') to include the UK in the list of authorised destinations for the export of dual-use goods after a hard Brexit, alongside other perceived 'safe' destinations, the US and Canada.

The UK's Department for International Trade ('DIT') and Export Control Joint Unit ('ECJU') has also published guidance to exporters indicating that in the event of a 'no-deal' Brexit, it would publish a new open general export licence in advance of the UK leaving the EU, with attendant information on registration and use.

UK politicians are unable to come to an agreement on the terms of the country's withdrawal from the EU.

UK sanctions strategy – what's the plan?

Speaking before a UK parliamentary committee hearing ('Global Britain: the future of UK sanctions policy inquiry'), Tom Keatinge, fellow of the Royal United Services Institute ('RUSI'), told committee members that while written evidence provided by the Foreign Office on sanctions after Brexit included 'standard phrases about sanctions being an extension of foreign policy and part of a "tool-kit"' that we're used to hearing from all governments', in terms of 'What is the strategy? What are we trying to achieve? That's not clear at this stage.'

Much, he said, would turn on the future of London's finance hub: 'The UK offers a particular lever to the European Union – which is the City of London. The question is, how are we going to use the financial power of this country once we're out of the European Union. Of course, London will remain one of the biggest financial centres in the world. Therefore, if you believe that financial sanctions are a powerful tool, we have one of the most powerful sanctions tools in the world following Brexit. But how do we plan to use that? And more generally, how will we employ economic statecraft?'

In its written statement, the UK Foreign Office said: 'At the international level, the UK will continue to seek multilateral cooperation on sanctions in response to shared threats, given that a collective approach to sanctions achieves the greatest impact. This will include significant contributions to the development of UN sanctions.

'The UK will look to remain a close partner of the EU on sanctions. As the Prime Minister set out in her speech at the Munich Security Conference on 17 February 2018, "[W]e will all be stronger if the UK and EU have the means to cooperate on sanctions now and potentially to develop them together in the future."

'Beyond the EU, the UK will also develop closer cooperation on sanctions with its allies and partners active in the use of sanctions, including, but not limited to, the United States, Canada and Australia. The United States, for example, is already a vital partner for the UK on sanctions, with extensive coordination already in place. There is also the potential for the UK to leverage its strong bilateral and multilateral relationships to bring together small groups of like-minded countries to agree joint proposals on sanctions.'

Links and notes

See here for the EU's contingency plan:
http://europa.eu/rapid/press-release_IP-18-6851_en.htm

See here for details of EU's proposed amending Council Regulation (EC) No 428/2009 by granting a Union General Export Authorisation for the export of certain dual-use items from the Union to the United Kingdom of Great Britain and Northern Ireland:
https://ec.europa.eu/info/sites/info/files/891_2_en_act_part1_v7.pdf

See here for UK government's guidance on exporting controlled goods in event of 'no-deal' Brexit:
https://www.gov.uk/government/publications/exporting-controlled-goods-if-theres-no-brexit-deal/exporting-controlled-goods-if-theres-no-brexit-deal

See here for Foreign and Commonwealth Office written evidence:
http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/foreign-affairs-committee/global-britain-the-future-of-uk-sanctions-policy/written/94581.html

WorldECR welcomes your news. Email the editor: tom.blass@worldecr.com

Need a second opinion?

In compliance-conscious times, it's only natural that companies should look beyond their own capabilities and seek advice from external advisers. But in what circumstances should they be doing so? And how can they ensure they're getting their money's worth? *WorldECR* explores.

Back in December 2018, US Treasury Under Secretary Sigal Mandelker gave a wide-ranging speech at the American Bar Association's Financial Crimes Enforcement Conference in which, amongst other themes, she elaborated on the Treasury's expectations of companies' compliance efforts.

Over the years, she said, the Treasury had seen 'the types of best practices that lead to strong and effective compliance programmes. We have also seen where entities fell short…'

Mandelker proceeded to outline what she considered to be the hallmarks of strong compliance, including senior management commitment, frequent risk assessments, and ensuring that 'all relevant personnel receive tailored training on OFAC obligation and authorities in general and the compliance programme in particular.'

And yet the compliance 'ask' increasingly gets tougher. As Mandelker's erstwhile colleague John E Smith (formerly director of OFAC and now a partner at the law firm Morrison & Foerster) says: 'In my experience, companies want to try to do the right thing. Where they're falling down is not generally out of willfulness, but because they're not paying attention to their supply chains and distribution chains or financial arrangements. In other words, they're not matching their commercial growth with their compliance efforts.'

Nowhere did Mandelker's speech describe circumstances in which there is an obligation or expectation to hire the services of external counsel or other third-party advisers – indeed, outside of settlement or consent agreements or where a company believes it may have committed a violation, there are none.

Nonetheless, engagement with outside counsel or consultants is seen by most companies as a *sine qua non* of their compliance programme, albeit that there exists no prescriptive template for managing that relationship. But is it best practice?

Deep pools

The pool of compliance expertise to draw on is broader and deeper than it has ever been.

'The evolution of modern compliance dates back to the 2002 Sarbanes-Oxley Act,' says Daniel Chapman, CEO at Texas-based consulting firm Presyse – Compliance Systems and Expertise. 'That brought many practitioners into the field. More than 15 years later, we have for the first time a group of extremely experienced compliance professionals.'

Sarbanes-Oxley raised the bar for board oversight over corporate financial statements and introduced stricter penalties for fraud. The focus of successive US administrations on national security following 9/11 and the growing use of targeted sanctions has shone a spotlight on compliance as a career – which can flourish, as readers of *WorldECR,* who make up much of that community, will know – in everything from one-, two- or three-partner boutiques operating from office suites in Austin, Amsterdam or Abu Dhabi to big-name, do-it-all corporate powerhouses on K Street or Canary Wharf.

But who, when and why should they be called in to advise?

For private practice advisers, says an experienced international trade lawyer, the following is a familiar scenario: 'OFAC (say) announces some major designations, or there's the announcement of a new executive order, and all of a sudden, we get client calls from companies suddenly worried about their exposure in a particular part of the world, or their relationship with a company or borrower. They want the reassurance, and they want a

second opinion…Or, there's a deal on the table, and just before they sign off and crack open the champagne, they want to be doubly sure that it's all compliant.'

That 'need for reassurance' may cloak disagreements and uncertainties between internal elements within the company – or oneself.

One senior compliance official within a US defence company told *WorldECR* that, in her experience, 'There's a number of aspects to consider when it comes to engaging external counsel. One is about looking inward, and asking yourself when you need help, by which I mean, knowing when you're up against the edge of your knowledge and experience, and recognising your limitations.

'It's also dependent on how your position and authority are viewed in the company. Some people have the gravitas – and the respect of management – which is sufficient to say, "I know the path forward." But if you don't, it may be that they want that expertise bought it.'

The structure of the company also has a significant bearing, she points out. 'For example, if trade compliance reports directly to senior leadership, then trade compliance may make that kind of decision. But if it reports to the legal department – it's left to "legal" to decide. And sometimes, where you've said, "Hold your horses", the commercial department will say they want a second opinion from a lawyer because they want the deal to go through.'

What external advisers can offer

External advisers can provide comfort in situations where the judgement of the business may be called into question in the future; to advise on whether certain goods can be exported to Iran, for example. They can 'sign off' the results of an in-house investigation, to reassure shareholders and mitigate risk – and provide specialist knowledge to complement the understanding of the general counsel or compliance team.

'In-house counsel may have a thorough understanding of the Russia sanctions, for example,' says Sheppard Mullin partner Reid Whitten, 'but when a question on EAR encryption comes around, they may decide that this needs to be checked out.'

And, as one highly experienced compliance manager in the defence industry notes, 'What you need is someone with very specific expertise, who knows the regulator well, who is not going to just read the regs at me.'

But our compliance official (who did not want to be named in this article) cautions against the 'cronyism' of the legally qualified who may regard themselves as a cut above the non-legally qualified, but highly experienced compliance personnel: 'A frustration is that where external counsel has been chosen by the legal department "to assist you", sometimes, they don't actually know a great deal about trade compliance. It's just that the legal team always uses a particular firm for M&A or HR or something else. It can be really annoying. Sometimes the legal department is just heavily biased toward anyone with a law degree (regardless of their actual knowledge of sanctions or export controls) and against even highly experienced compliance people. What I really don't need is someone to come along and read the regs to me, when I've been living and breathing them for years.'

'What I really don't need is someone to come along and read the regs to me, when I've been living and breathing them for years.'

But, she says, good advice from experienced practitioners is invaluable, 'in specific, but also more general ways – such as benchmarking'. So, 'It's hard to ask peers in other companies, "What are you discussing with regard to Iran?" But you can ask an outside lawyer, "What's standard practice in other companies?" And even though they're bound by attorney-client privilege, they can give you the insight that comes with having worked across a range of businesses.'

Large international businesses will often assemble a panel of law firms to advise on different compliance functions, taking into account considerations such as the synergy between in-house counsel and private practice partners; inside knowledge and relationships with the regulator; the need for a particular specialisation; and the value of fielding a firm with an awe-inspiring reputation if things get sticky.

'I make sure that we have all the tools in the toolbox available,' says John Pisa-Relli, managing director of global trade compliance at Accenture. 'If that means going outside the panel to get the best advice, we will ensure that we can do that.'

Of course, not all third-party advice comes from law firms. Consultancies, large and small, supply a range of needs. They may offer lower costs and the flexibility to advise on smaller projects – or, conversely, advise and implement major compliance programmes or the procurement of compliance tools which law firms are often not equipped to undertake.

In either case, distinctions are increasingly blurred: lawyers move easily from law firms to 'consultancies' where they undertake roles that are pretty much inseparable from their former employment, while law firms themselves take on non-legally qualified consultants as trade advisers or directors. At the end of the day, it's the experience that counts.

Meanwhile, the growth in competition, commensurate with perceived risk and higher penalties, does raise the bar for all involved.

'The clients are more sophisticated, the work is more difficult,' says Daniel Martin, partner at UK law firm HFW, which advises the shipping, commodities, aerospace and insurance sectors.

Firms have to go beyond the traditional service mile. Inducements can include cut-price due diligence to regular clients, who have to evaluate whether it is worth incurring the cost of compliance for a transaction to pass muster. Martin suggests that providing a 'cradle-to-grave' service spanning everyday compliance to investigations fosters confidence in external counsel, and that it will, in turn, lead to a thorough understanding of the client's business.

Another incentive is face-to-face in-house training, tailored to cover developments that affect each particular business. 'We find this more effective in an era in which the volume of client alerts and briefings risks information overload,' says Martin. Clients expect anticipatory rather than responsive advice: 'They really value it when trade lawyers alert them to changes that are about to happen,' says Whitten.

Who is the best point of contact in the business?

Views are mixed on whether the point of contact for external counsel should be the in-house legal team. 'If the nature of the business is highly commoditised so that the legal context has been addressed already, then it is possible to liaise with a client manager who has no legal role,' says Martin.

Others argue that legal questions and regulatory discussions should only take place between legal specialists 'to avoid misinterpretation and ensure a streamlined communication.'

'Nonetheless, in order to manage cross-functional topics or work on evaluating certain business projects, representatives from programme management or procurement may be embedded into the dialogue – led by trade compliance,' says Alex Groba, director of foreign trade at MTU Aero Engines.

Easy as ICP?

All those spoken to for this article – trade compliance managers, consultants, private practice lawyers, in-house counsel – agree that external legal providers have a vital role in advising on building a successful internal compliance programme ('ICP').

'Considering the evolving requirements and, more than ever, the importance of a comprehensive internal rule set, establishing an ICP goes far beyond ensuring appropriate classifications and shipment/technology controls,' says Groba.

'A mixed team of lawyers and consultants may be a wise choice, as long as roles and responsibilities have been clearly defined.'

The downside? A lack of knowledge of the internal business culture of the company may mean that proposed policies and procedures will not function well in practice.

'External legal counsel does not have the experience to develop a pragmatic compliance programme unless they have been in-house,' argues Chapman. 'They may not understand R&D, finance, logistics. When you are building internal controls, you must have solid expertise. An over-reliance on external counsel can mean the processes are not fit for purpose and may result in a major violation.'

Groba points to the need for a 'detailed understanding of a company's internal processes', how they fit into the ICP as well as 'a climate of mutual trust between the trade compliance team and other departments,' without which 'external counsel will just cost money but will not improve overall compliance,' he says.

'A mixed team of lawyers and consultants may be a wise choice, as long as roles and responsibilities have been clearly defined,' says Groba.

Whether to work with a range of legal specialists, or trust one or two firms, is a decision each business has to take on its own. 'In the end what is important is a deep understanding of the individual business model to ensure legal advice is tailored to the customer, instead of general regulatory explanations,' says Groba.

Tank Talk

News and research from the export control, non-proliferation and policy world

Failed missile launch 'wrong target of international outrage' – IISS

Writing for the Institute of International Security Studies ('IISS'), fellow Michael Ellerman notes that on 15 January, Iran 'attempted and failed to lift the Payam-e Amirkabir satellite into orbit using a Simorgh rocket'. Israeli prime minister Benjamin Netanyahu and US secretary of state Mike Pompeo both responded by describing the attempt as being in violation of international agreements and UNSCR 2231.

As Simorgh was a satellite launch vehicle ('SLV') and not an intercontinental ballistic missile ('ICBM') there was no breach of Resolution 2231, argues Ellerman, adding that that's not to say that there aren't risks attached to Iran's rocket programme. The prospect of a launch, he says, of the Khorramshahr missile – which uses propellants that are more energetic than those employed by Scud and Nodong systems, 'is of much greater concern. The higher energy propellant combination allows engineers to reduce significantly missile size and mass, which in turn could form a basis for a road-mobile, nuclear-capable ICBM.'

Similarly, in the event of the 'restart of the two-stage, solid-fuel Sajjil missile, which has not been flight tested in eight years,' the international community would also 'be right to protest, as such developments could be exploited to fashion a nuclear-tipped ICBM.' But for now, 'diplomatic capital should not be diluted by protesting Iran's use of the Simorgh SLV but should instead focus on Iranian actions that pose the greatest risk to international security.'

https://www.iiss.org/blogs/analysis/2019/01/iran-satellite-launch

North Korea's dual-use capability and collaboration

In an occasional paper published in December by the James Martin Center for Nonproliferation Studies ('CNS)', Joshua Pollack and Scott LaFoy examine the efforts that Kim Jong Un has made to develop indigenous technologies to bypass international sanctions, so as to reduce North Korea's need for imported goods.

They explain: 'To assess the extent of this activity, and to identify collaborative research involving dual-use technologies and other technologies of potential military significance [they] developed a new dataset capturing publications co-authored by North Korean scientists and foreign scientists between 1958 and April 2018 ... Based on an initial evaluation, at least 100 published articles jointly authored by North Korean and foreign scientists have identifiable significance for dual-use technology, weapons of mass destruction or other military purposes. Areas of concern or potential concern include:

- Uranium purification (Romania, 1991–92)
- Insulation of high-voltage cables for nuclear power plants (China, 2007-12)
- Materials science with a potential nuclear application (China, 2012)
- Damping technology applicable to space/missiles (China, 2016-17)
- Mathematical modeling applicable to space/missiles (China, 2006-16)
- Special heavy vehicles and production systems (China, 2011-16)
- Precision machine tools (China, 2016)
- Carbon composites (China, 2012)
- Other materials science with potential military applications (China, 2011-18)
- Optical tracking and image parsing (China, 2011-16)
- Remote sensing and satellite-imagery processing (China and United States, 2010-13)
- GPS-related work (Germany and China, 2007 and 2016)
- Laser and plasmonics research (Germany and China, 1998-2016)
- Biological research potentially of a dual-use character (China and Australia, 1987-2017)
- Cybersecurity (China, 2012)

Some of these activities, they say, 'may be contrary to provisions in international and national sanctions regimes. UN Security Council resolutions forbid the provision to North Korea of "technical training, advice, services, or assistance" related to a list of banned items that includes dual-use and military-related "technology." ... The sanctions regime may therefore provide leverage against the continuation of some areas of collaborative research.'

www.nonproliferation.org/op43-north-koreas-international-scientific-collaborations-their-scope-scale-and-potential-dual-use-and-military-significance/

How should crypto community respond to recent OFAC designations?

Writing for the Royal United Services Institute ('RUSI'), Kayla Izenman explores how the 'crypto community' – i.e., virtual currency exchanges – might or should respond to the designation last year of two Iranians for their role in the SamSam ransomware campaign.

On the one hand, she writes, the 'strong message' from OFAC may drive the community underground. On the other: 'Blockchain analysis companies, such as Chainalysis and Elliptic, already provide intelligence to help companies meet their "Know Your Customer" and anti-money laundering compliance obligations and enable better understanding of suspicious crypto transactions. By utilising this technology, together with other innovative solutions, centralised exchanges are in prime position to regulate the blockchain themselves, to some extent.'

One solution, Izenman suggests, 'lies in the possibility of "tainted" coins, a concept in which stolen or designated coins are tagged as they move through the system, indicating the flow of money laundering as well as keeping exchanges and crypto users safe from inadvertently violating sanctions.'

Such a change would, she says, 'require incredible effort, desire, and expense on the part of the exchanges and developers,' but she argues that 'with crypto's already rocky reputation as a facilitator of crime, it could be in the community's best interest to deal with its own problems.'

Enough already

WorldECR speaks with Brad Brooks-Rubin, Managing Director of the Enough Project and The Sentry, and finds out how the advocacy organisation seeks to employ the tools of state in its pursuit of peace and justice in Africa.

Brad Brooks-Rubin says that he sometimes feels 'like a one-man multi-stakeholder initiative', reflecting a career that has seen him bring his legal skills to bear in government (at both the departments of State and the Treasury), in an industry association (the Gemologicial Institute of America), in private legal practice (at LeBoeuf, Lamb, Greene & Macrae and Holland & Hart), and now for the Enough Project, where he is managing director of an advocacy group that seeks to use sanctions tools in a way that is pretty much unique, and in a part of the world – sub-Saharan Africa – the conflicts of which are too often misunderstood or ignored.

But his previous experiences and the insight gained from them are now proving invaluable in his work at the Enough Project.

'When I was a counsel at OFAC, my portfolio was sub-Saharan sanctions. Traditionally, we just put people on a list. In the late 2000s, we began developing the template for more effective sanctions – because you can't just put people on a list and hope it has an effect.'

The key to success, he says, lies in identifying networks and choosing the right targets.

'Before, you'd just pick on some people. But there's no point in doing that if they don't have any assets, or they do have assets but you don't know where they are.'

Brad Brooks-Rubin is managing director at the Enough Project, which supports peace and an end to mass atrocities in Africa's deadliest conflict zones, and The Sentry, which 'follows the money in order to create consequences for those funding and profiting from genocide or other mass atrocities in Africa, and to build leverage for peace'.

From 2009-2013, he served as the Special Adviser for Conflict Diamonds at the US Department of State, where he provided working-level representation for the United States in the Kimberley Process. He also contributed to US efforts related to conflict minerals in eastern Congo. Prior to that, he served as an attorney-adviser at OFAC and in private legal practice.

A different approach

The origins of the Enough Project lie in the Darfur crisis, and in work that founders John Prendergast and Gayle Smith (now president of poverty-eradication campaign group, The ONE Campaign) were doing at the International Crisis Group and the Center for American Progress, respectively.

Where the Enough Project brought something new in its response to crises – conflicts playing out, and atrocities committed, in East and Central Africa – was, says Brooks-Rubin, in recognising that the approach hitherto taken by many governments and NGOs wasn't working.

'The traditional tools of diplomacy are largely about finger wagging. But we knew these armed groups, who were committing the atrocities, and we knew that they were making a lot of money, and that peace for peace's sake was not in their interests.'

The late 2000s, he points out, saw tools such as the AML regime being used more politically. 'We realised that if they were directed in more specific ways, they would have more impact – and we began not only to advocate for those tools being applied most effectively, but also to provide the information that would enable government to do so.'

In 2015, John Prendergast co-

founded with the actor George Clooney a sister project to Enough called The Sentry, an investigative team including policy analysts, forensic investigators and regional experts who 'follow the money' to 'create consequences for those funding and profiting from genocide or other mass atrocities in Africa'.

'The US government isn't able to focus sufficient resources on collecting the evidence,' says Brooks-Rubin. 'But we are providing the government, and the European Union, with information. Which means that they have the information they need to replicate the network-based approach, as they've done with North Korea and Iran, to create leverage that results in behaviour change. And we know that that's a strategy that works, of course, because of the massive penalties that are in place.'

Countries and areas of particular concern to the Enough Project include the Central African Republic, Democratic Republic of Congo, Sudan, and South Sudan. None of these are on the corporate compliance agenda in the same way as Russia, Iran or North Korea, but, Brooks-Rubin points out, 'When US Under-Secretary [Sigal Mandelker] visits East Africa (as she did in June last year with John Prendergast – on a visit that saw Mandelker raise concerns about illicit money flows out of South Sudan and into the coffers of its neighbours) the banks are definitely taking note. Of course, we can't always guarantee everything, but the playbook works. And the government is now asking us: "Who are the people that matter?"'

The Enough Project

The Enough Project was founded by John Prendergast with Gayle Smith in 2007. Prendergast, who remains its Founding Director, had previously worked for the Clinton White House, the State Department, two members of Congress, the National Intelligence Council, UNICEF, Human Rights Watch, the International Crisis Group, and the US Institute of Peace.

The Project's intention is to 'counter armed groups, violent kleptocratic regimes, and their commercial partners that are sustained and enriched by corruption, criminal activity, and the trafficking of natural resources.'

In 2016, with actor George Clooney, Prendergast co-founded The Sentry – a team of forensic investigators dedicated to 'following the money…to create consequences for those funding and profiting from genocide or other mass atrocities in Africa,' guided by the dictum that 'War crimes shouldn't pay.'

Brad Brooks-Rubin serves as the Managing Director at Enough. He joined Enough from the Gemological Institute of America (GIA), where he served as the first Director, Global Development and Beneficiation.

'The US government isn't able to focus sufficient resources on collecting the evidence…But we are providing the government, and the European Union, with information.'

Brad Brooks-Rubin

Back in September 2017, OFAC designated three people and three companies under Executive Order 13664 ('the South Sudan order') 'for actions or policies that threaten the peace, security, or stability of South Sudan'. This coincided with the publication of an advisory by the Treasury's Financial Crimes Enforcement Network ('FinCen') reminding banks that 'OFAC and UN designations increase the likelihood that other, non-designated South Sudanese senior political figures and opposition leaders may seek to protect their assets, including those that are likely to be associated with political corruption, to avoid potential future blocking actions. Consistent with existing regulatory obligations, financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with South Sudanese corruption.'

In December 2017, Israeli billionaire Dan Gertler was sanctioned with the release of a new Global Magnitsky executive order issued by President Trump, while the Treasury Department simultaneously designated 19 companies and one individual associated with Gertler. OFAC describes Gertler as having 'amassed his fortune through hundreds of millions of dollars' worth of opaque and corrupt mining and oil deals in the Democratic Republic of the Congo (DRC),' and who has close ties to DRC president Joseph Kabila. OFAC followed up on this action in June 2018 when it sanctioned 14 companies 'owned or controlled by Gertler' under the Global Magnitsky executive order.

In December 2018, OFAC sanctioned three individuals and six entities under Executive Order 13664. Two of the individuals, Gregory Vasili and Obac William Olawo, are South Sudanese, designated 'for being leaders of entities whose actions have the purpose or effect of expanding or extending the conflict in South Sudan'. The third, Israel Ziv, is a retired Israel Defense Forces major general, who, according to OFAC, used an agricultural company as cover for the sale of $150 million-worth of weapons into South Sudan.

'It's imperative to understand the value chain and the supply chain,' says Brooks-Rubin, 'whether that's in relation to conflict minerals or oil, the UN Guiding Principles or the Dodd-Frank Rule. Because often you'll find that these people are all connected. If you're doing business in minerals in Congo, you're probably dealing with a corrupt actor. And that means it's also your problem.'

Another implication is that – given that corruption and human rights violations are increasingly on the sanctions agenda – the fact that, for example, Sudan (as distinct from South Sudan) is no longer under embargo doesn't mean it's now 'carte blanche to do business there.'

The $60bn plan

Any discussion of Sub-Saharan Africa's future is, of course, meaningless without including China's ambitions on the continent (not least, given President Xi's September 2018 promise of $60bn worth of support and investment), all of which may soon overshadow the West's assumption that it plays a leadership role.

'Yes, China is a major factor – and a really interesting test case for exploring how far we can go with this pressure and strategy. Of course, there's nothing inherently wrong with Chinese investment and support in Africa. But if it has allowed people like [Sudanese president] Omar al-Bashir and Joseph Kabila [who stepped down from the presidency of the DRC last year] to stay in power for so long, and as we start getting closer to the link between corruption and power, should we step back? The United States has sanctioned Chinese entities before in different contexts [i.e., under the North Korean sanctions programmes]. Perhaps we'll find that [imposing sanctions on Chinese companies for links to African corruption] is a step too far.'

'What would help would be if the European Union were to apply corruption as a designation criterion…There are plenty of targets available, and that would add to the effectiveness.'

Brad Brooks-Rubin

Pushing things forward

What is clear, says Brooks-Rubin, is that despite some of the periodic publicity about the ability of the current US administration to function smoothly (and personality clashes and other controversies), in this regard at least, things are moving forward.

What the process that culminated in the Joint Comprehensive Plan of Action proved, Brooks-Rubin suggests, is that sanctions can be used to encourage an ongoing transition:

'If you look back at the P5+1 negotiations, the Treasury would continue to ratchet up the pressure even when there was progress. They were saying in effect, "We're taking this action against Iran because we're taking these negotiations seriously and we want to show there's a lot at stake."'

There's no reason why, he says, such a model (notwithstanding whatever one may think of the deal agreed, and the US pull-out) shouldn't be used in dealing with African warlords.

Last September, John Prendergast addressed a UN Security Council session on the 'devastating link between corruption and conflict,' where he told delegates that sanctions imposed on individuals in Africa were typically upon 'too few individuals sanctioned too infrequently,' because, 'the mandate does not exist to target those responsible for the corruption, those at the centre of the networks responsible for greed-fueled extreme violence and their commercial collaborators. Over time, and in the absence of meaningful enforcement, warring parties have come to regard these kinds [of] erratically applied, one-off sanctions as a vague annoyance for their public relations rather than as a serious threat to their power.'

At a joint press conference with both Prendergast and US Treasury assistant secretary Marshall Billingslea (recently nominated to be an under secretary of state), then-US ambassador to the United Nations Nikki Haley told reporters that the US would continue to press the Security Council to recognise the importance of tackling corruption.

For his part, Billingslea described the recommendations that Prendergast (whom he described as 'a close partner') made to the Security Council as 'very much in line with how the Administration and the Treasury' are approaching the issues.

'We very much welcome the chance to explore further opportunities,' he said, 'to engage in targeted financial sanctions, going after the complete networks' of those who are 'extorting or extracting wealth from the helpless.'

These are laudable and ambitious objectives – and long overdue. And recent designations of Central American entities show that the US government is now comfortable using corruption as a criterion for inclusion on a sanctions list. But where does the trajectory cross paths (or otherwise) with the other hallmark of this administration's approach to foreign affairs: its willingness to 'go it alone' and apparent distaste for global consensus?

'The leverage is always increased if it's multilateral,' says Brooks-Rubin. 'Certainly, the European Union and the United Kingdom are very important – they're sending senior diplomats to the region. What would help would be if the European Union were to apply corruption as a designation criterion… There are plenty of targets available, and that would add to the effectiveness.'

He adds further food for thought: 'There's potentially a huge opportunity here as the UK develops its own sanctions regime if it leaves the European Union.'

Warlords, cronies and carpetbaggers be warned.

More information about the work of the Enough Project and The Sentry can be found at:

www.EnoughProject.org and **www.TheSentry.org**

WorldECR welcomes your feedback. Email the editor: tom.blass@worldecr.com

EU

First listings under EU's Chemical Weapons sanctions regime

By Maya Lester QC, Brick Court Chambers

www.europeansanctions.com

The EU has added nine individuals and one entity to its Chemical Weapons sanctions list (asset freeze and travel ban). These are the first listings to be made under the sanctions regime. (See Council Decision (CFSP) 2019/86, Council Implementing Regulation (EU) 2019/84, and EU Press Release.)

Syria-based Scientific Studies and Research Centre ('SSRC') was sanctioned for the 'development and production of chemical weapons'. The entity is already listed under the EU's Syria sanctions regime.

The nine listed people are: Tariq Yasmina; Khaled Nasri; Walid Zughaib; Firas Ahmed; Said Said; Anatoliy Vladimirovich Chepiga; Alexander Yevgeniyevich Mishkin; Vladimir Stepanovich Alexseyev; and Igor Olegovich Kostyukov.

Mr Chepiga and Mr Mishkin (both Russian GRU officials), and Mr Kostyukov and Mr Alexseyev (the Head and First Deputy Head of the GRU, respectively), were sanctioned for being 'responsible for [the] possession, transport and use in Salisbury (UK) of a toxic nerve agent' against Sergei and Yulia Skripal (March 2018). The other five listed people are 'Syrian officials directly involved in the SSRC's activities'.

Council Decision (CFSP) 2019/86: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0086&from=EN

EU Press release: https://www.consilium.europa.eu/en/press/press-releases/2019/01/21/chemical-weapons-the-eu-places-nine-persons-and-one-entity-under-new-sanctions-regime/pdf

EU

EU adds individuals and entities to Syria sanctions

By Michael O'Kane, Peters & Peters

www.europeansanctions.com

On 21 January, the Council of the European Union added 11 businessmen and five entities to its Syria sanctions list, on the basis that they 'support and/or benefit from the Syrian regime' by being involved in 'luxury estate development and other regime-backed projects'. They will now be subject to EU-wide asset freezes and (where appropriate) travel bans.

The 11-listed businessmen are: Anas Talas; Nazir Ahmad JamalEddine; Mazin Al-Tarazi; Samer Foz; Khaldoun Al-Zoubi; Hussam Al-Qatirji; Bashar Mohammad Assi; Khaled al-Zubaidi; Hayan Mohammad Nazem Qaddour; Maen Rizk Allah Haykal; and Nader Qalei.

The five listed entities are: Rawafed Damascus Private Joint Stock Company; Aman Damascus Joint Stock Company; Bunyan Damascus Private Joint Stock Company; Mirza; and Developers Private Joint Stock Company.

Council Implementing Decision (CFSP) 2019/87: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0087&from=EN

Council Implementing Regulation (EU) 2019/85: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0085&from=EN

EU Press Release: https://www.consilium.europa.eu/en/press/press-releases/2019/01/21/syria-eu-adds-eleven-businessmen-and-five-entities-to-sanctions-list/pdf

WorldECR welcomes your bulletins. email tom.blass@worldecr.com

USA

Enforcement action round-up

By Kevin Petrasic, Paul Saltzman, Nicole Erb, Jeremy Kuester, Cristina Brayton-Lewis and John Wagner, White & Case

www.whitecase.com

Enforcement actions taken by the Office of Foreign Assets Control ('OFAC') in late November/December 2018 included:

Settlement with US holding company for apparent violations of Belarus sanctions

On 20 December 2018, OFAC announced a US$7.8 million settlement with a US holding company to settle potential civil liability for 26 apparent violations of the Belarus Sanctions Regulations.[1] OFAC found that between 18 January 2012 and 27 October 2015, the holding company and/or one of its US subsidiaries violated the Belarus Sanctions Regulations by approving 26 purchases of a chemical from a Belarusian SDN. In addition, the holding company's Hungarian subsidiary also purchased the chemical from the SDN, with the approval of senior executives of the holding company. OFAC considered the following aggravating factors:

i. the holding company acted with reckless disregard for US economic sanctions requirements and/or failed to exercise a minimal degree of caution or care in avoiding the conduct that led to the apparent violations and failed to incorporate OFAC compliance checks in its overall risk mitigation strategy;
ii. personnel, including senior and executive-level managers, were aware of – and participated in – the conduct that led to the apparent violations;
iii. the holding company approved the Hungarian subsidiary's purchase of a significant volume of chemicals from the SDN for a period of several years, resulting in significant harm to the sanctions programme objectives and conferring more than US$18 million to a Belarusian government entity;
iv. the holding company and US subsidiary are large entities that engage in a significant volume of international trade and cross-border transactions; and
v. specifically for action after February 2015, senior personnel actively discussed US sanctions related to the SDN raised by third parties but did not review the company's US legal obligations and continued to approve SDN transactions.

OFAC alleged that the company knew or had reason to know that items in some of the shipments were ultimately intended for Iran.

OFAC considered the following mitigating factors:

(a) neither the holding company nor its US subsidiary received a penalty notice or finding of violation from OFAC in the five years preceding the earliest apparent violations;
(b) the holding company and US subsidiary cooperated with OFAC's investigation, including by voluntarily self-disclosing the apparent violations, providing detailed and well-organised information for OFAC's review, and by agreeing to toll the statute of limitations for a total of 643 days; and
(c) the holding company and US subsidiary confirmed that they have terminated the conduct that led to the apparent violations and have taken steps to minimise the risk of recurrence of similar conduct in the future.

Settlement with Chinese oil and gas company for apparent violations of Iran sanctions

On 12 December 2018, OFAC announced a US$2.8 million settlement with an oil and gas company based in China for 11 apparent violations of the Iranian Transactions and Sanctions Regulations ('ITSR'), concurrent with a separate settlement between the company and BIS.[2]

According to OFAC, the company exported or re-exported, or attempted to export or re-export, US-origin goods ultimately intended for end-users in Iran by way of China and the UAE.

OFAC alleged that the company knew or had reason to know that items in some of the shipments were ultimately intended for Iran.

OFAC considered the following aggravating factors, among others:

i. the company wilfully violated the ITSR by engaging in and systematically obfuscating conduct it knew to be prohibited by company policy and economic sanctions, and continued to engage in such conduct even after the US government began to investigate the conduct;
ii. employees, including several management-level personnel, had contemporaneous knowledge of the transactions in question;
iii. employees took actions to conceal the nature of the transactions from the US government; and
iv. the company falsified information

Links and notes

[1] https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181220_zoltek.pdf

[2] https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181212_jereh_settlement.pdf

on electronic export filings and made other false statements to the US government in the course of the investigation.

OFAC also considered the following mitigating factors:

(a) the company has no prior sanctions history with OFAC;
(b) the company cooperated with OFAC's investigation by disclosing possible violations involving other sanctions programmes and responding to OFAC's requests for information regarding Iran;
(c) the company agreed to toll the statute of limitations; and
(d) the company took remedial steps and corrective actions to prevent a recurrence of the apparent violations.

USA

Screening the use of screening software for OFAC sanctions compliance

By Christopher R. Brewster, Chris Griner, Gregory Jaeger and Bibek R. Pandey, Stroock

www.stroock.com

On 27 November 2018, the Treasury Department's Office of Foreign Assets Control ('OFAC') announced a settlement agreement with a Virginia-based global technology and services company operating in the aviation, electronics, communications and defence sector. The settlement concerned apparent violations of the Ukraine Related Sanctions Regulations, 31 C.F.R. part 589. According to the settlement agreement, the company had shipped products through its distributors in Canada and Russia to an entity in Russia that, although not identified on OFAC's List of Specially Designated Nationals and Blocked Persons ('SDN List'), was majority owned by an SDN entity. The company relied on third-party software to screen its counterparty, but the software failed to generate an alert for the subsidiary. OFAC's announcement appears intended to raise a number of compliance lessons relating to the use of, and reliance on, third-party screening software for OFAC sanctions compliance.

First, the decision makes clear that screening software must be sufficiently robust to screen the counterparty as well as entities on its corporate structure against the SDN List (including potential matches to persons/entities with close name variations).

Under OFAC guidance (the '50% Rule'), an entity that is not listed on the SDN List but is majority owned, either directly or indirectly, in the aggregate, by a designated person or entity (or group of sanctioned parties) is also subject to blocking sanctions. US persons are prohibited from dealing with such an entity. The screening software should also screen for any designated individuals acting as an officer or director of the counterparty, even if the counterparty is unlisted. If such designated persons are involved in the transaction, the transaction could be subject to OFAC sanctions.

The settlement argues that in-house export control professionals should understand not only the functionality, but also the risks of relying on third-party screening software.

Second, however good the software may be, an exclusive reliance on automation is not a sufficient compliance strategy. OFAC took note that the company failed to recognise 'warning signs' when exporting the goods to 'the subsidiary of a blocked person with *nearly the same name* as the blocked person.' [Emphasis added.] The near-identical name between the counterparty and its designated parent, in OFAC's view, should have raised red flags to the export control specialist reviewing the transaction, particularly since the company was 'large and sophisticated' with prior violations of OFAC sanctions. Thus, the settlement argues that in-house export control professionals should understand not only the functionality, but also the risks of relying on third-party screening software.

Finally, the OFAC settlement encourages a risk-based approach, using business intelligence tools to conduct enhanced due diligence on high-risk transactions. The additional cost of employing such enhanced due diligence can be justified for high-value transactions involving high-risk jurisdictions such as Russia, Syria and Venezuela. In that regard, OFAC's expectation is that a company's compliance unit will receive adequate resources, including human capital, IT and other resources as appropriate.

But here again, software is not a total solution. Where there are signals that a company may be related to a sanctioned party, OFAC plainly expects US trading partners to inquire further. Nor is a party necessarily in the clear because a sanctioned party's interest in a potential trading partner falls short of 50%. In such cases, it may well make sense to take additional steps to ensure that the sanctioned party will have no role in, and will not benefit from, the transaction. Absent such assurances, the prudent course may be to walk away.

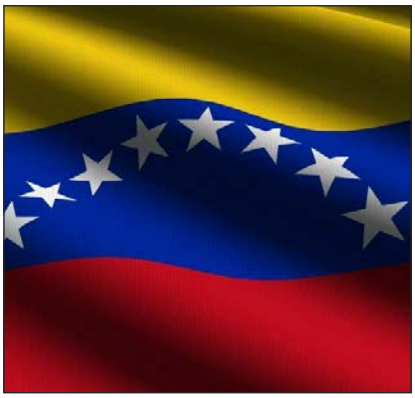
The settlement is at:
https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181127_metelics.pdf

USA

US government sanctions PdVSA and its subsidiaries

By Glen Kelley, Jacobson Burton Kelley PLLC

www.jbktradelaw.com



On 23 January, the recently elected President of the Venezuelan opposition-led National Assembly, Juan Guaido, declared himself the legitimate President of Venezuela citing provisions of the Venezuelan constitution. Immediately thereafter, in a pre-coordinated action, US President Trump stated that the US recognised him as such.

Several dozen other countries have recognised Guaido as, and stated that Nicolas Maduro is no longer, the legitimate President of Venezuela, citing grave concerns over the 2018 re-election of Maduro, the impoverishment of the Venezuelan people, and corruption within the Maduro government. Several EU countries have said they will recognise Guaido if Maduro does not call new presidential elections by 2 February 2019.

On 28 January, the US greatly expanded its economic sanctions on Venezuela to include broad 'blocking' (asset-freezing) sanctions on the national petroleum company Petróleos de Venezuela, S.A. ('PdVSA'), and its direct and indirect subsidiaries. There are dozens of significant PdVSA subsidiaries around the world, including CITGO in the United States.

With the PdVSA sanctions, the US government intends to support the efforts of the Venezuelan opposition, led by Guaido, to take control over Venezuelan government assets in the United States. The State Department announced that the PdVSA sanctions 'will preserve the core pillar of Venezuela's national assets for the people and a democratically elected government'.

Summary of the PdVSA sanctions

On 28 January, the US Office of Foreign Assets Control ('OFAC') announced that PdVSA had been added to the US List of Specially Designated Nationals and Blocked Persons (the 'SDN List'). Companies on the SDN List, and any entity in which they hold, individually or in the aggregate, a 50% or greater ownership interest, are covered by broad blocking (asset-freezing) sanctions.

As a result, companies formed under US law, US citizens and permanent residents and other entities or individuals ('persons') located in the US ('US persons') are generally required to freeze any assets owned by PdVSA and its subsidiaries, and any assets or funds in which they have any interest. US persons are also generally prohibited from engaging in any other types of transactions with or involving PdVSA or its subsidiaries.

This will impact a broad range of ongoing transactions and commercial relationships that involve US persons, US dollar payments or another 'nexus' (connection) to the United States.

The US government also issued several 'general licences' that provide for wind-down periods and authorise certain transactions that would otherwise be prohibited by the new blocking sanctions on PdVSA and its subsidiaries. A general licence describes certain types of transactions that are authorised for any party and any transaction that satisfy its terms.

These general licences do not authorise any transactions that would also be prohibited by the more limited pre-existing sanctions on Venezuela. The following are some of the broadest of these new general licences ('GLs'):

- **GL 7** authorises for six months, until 27 July 2019, transactions with certain PdVSA subsidiaries – CITGO Holding, Inc., PDV Holding, Inc., and their subsidiaries – that would otherwise be prohibited by the blocking sanctions on PdVSA. GL 7 does not authorise transactions involving any other PdVSA entity, except for certain petroleum imports to the United States (see GL 12, below).
- **GL 11** authorises US employees of non-US entities anywhere in the world other than the United States or Venezuela to participate in the 'maintenance or wind-down' of pre-existing PdVSA business, for two months, until 29 March 2019. GL 11 also authorises US banks to reject (rather than having to freeze) certain funds transfers between non-US persons that originate and terminate at non-US banks and involve PdVSA or one of its subsidiaries.
- **GL 12** temporarily authorises the continuation or wind down of imports of Venezuelan crude to the US and other business involving PdVSA. For one month, until 27 February 2019, GL 12 broadly authorises the 'wind down' of existing business with PdVSA or its subsidiaries that was underway as of 28 January 2019 (pre-existing PdVSA business). GL 12 authorises the purchase and importation into the United States of petroleum and petroleum products from PdVSA or its subsidiaries for three months, until 28 April 2019.

Unless authorised under another GL, any payment owed to PdVSA, or that would directly or indirectly benefit PdVSA, must be made into a 'blocked account' at a US bank, meaning a frozen, interest-bearing account reported to the US government. GL 12 does not authorise the transfer of any debt or equity in, to or for the benefit of' PdVSA or its subsidiaries or the exportation of diluents from the US to Venezuela.

Case by case (just in case)

'We're busy,' say not just the London law firms but many others in the EU, 'trying to second-guess Brexit.' Indeed, they have been since the result of the referendum in 2016 – and a good few have spent significant sums showcasing their expertise in an area of practice that is still defining itself.

Yes, there are definite things to be said about sanctions and export controls post-Brexit and how it all fits into the broader ecosystem of trade – well, as one sage said, 'If you've never jumped off a cliff before, it's impossible to lecture others on landing technique.'

But if Brits are waking up to the very real possibility of food shortages and price rises, they can at least comfort themselves with the thought that the situation is unlikely to deteriorate to the extent that it resembles Venezuela's, where rioting and violence currently reign and the emergence of a self-declared presidential alternative to Nicolas Maduro suggests that conflict will precede any political solution.

On the Venezuela question, it seems the European Union and the United States are of a similar mind. The country's plight is a result of the failed policies of Maduro and change is necessary and will be encouraged.

Talking of convergence, is Germany's prohibition of Mahan Air from landing at its airports also indicative that some in Europe are seeing things through Washington's eyes? Playing the Iranian terror card means EU Member States can crank up the pressure on Tehran without making concessions *vis a vis* the nuclear deal. Indeed, an announcement regarding the fabled Special Purpose Vehicle is thought to be imminent – but it will be accompanied by warnings for Iran about its global citizenship.

'If you've never jumped off a cliff before, it's impossible to lecture others on landing technique.'

It would seem that, in these confusing times, the best approach for business as it navigates the swirling waters of national security and realpolitik is to look at each challenge as a case unto itself, and not look too hard for patterns. Take the very recent removal of Rusal, EN+ Group and JSC EuroSibEnergo: The sanctions against the Deripaska-controlled companies created supply chain issues – and job losses – in the global aluminium markets. Who blinked first? The US government, afraid of continued disruption to the markets, or the companies, whose directors have successfully reduced Oleg Deripaska's control, so as to free themselves from the yoke of OFAC. And will the outcome set a trend?

Perhaps best not to read to much into it, just in case…

Tom Blass, January 2019
TNB@worldecr.com

OFSI gears up to use its civil enforcement powers



The Office of Financial Sanctions Implementation is the UK's new(-ish) financial sanctions authority. Eighteen months old, it's yet to use its civil enforcement powers. Rachel Barnes, Patrick Hill and Genevieve Woods consider why and what the future may hold.

The UK's Office of Financial Sanctions Implementation ('OFSI') is the UK's competent authority for implementing and enforcing financial sanctions. It has enjoyed powers to impose civil monetary penalties for serious breaches of financial sanctions since April 2017, yet in 18 months it has never exercised those powers. This article examines why that may be the case, why OFSI's approach may now be changing, and what the future may bring.

OFSI's first year: education and engagement

OFSI was established on 31 March 2016. The government's intent, set out in the 2015 Summer Budget, was that:

'The Office will provide a high-quality service to the private sector, working closely with law enforcement to help ensure that financial sanctions are properly understood, implemented and enforced. This will ensure financial sanctions make the fullest possible contributions to the UK's foreign policy and national security goals and help maintain the integrity of and confidence in the UK financial services sector.'

During its first year of operation, OFSI primarily focused on education and engagement. It issued guidance on compliance while its proposed enforcement powers progressed through parliament, in the form of the Policing and Crime Bill. Until that bill was passed, OFSI did not have the power to impose civil monetary penalties for breaches of financial sanctions and nor could appropriate sanctions cases be resolved by deferred prosecution agreements.

OFSI's second year: gaining new powers

The Policing and Crime Act 2017 ('the 2017 Act') came into force on 1 April 2017. Along with adding sanctions cases to the list of cases to which deferred prosecution agreements ('DPAs') can be applied, the 2017 Act gave OFSI new civil enforcement powers as an alternative to referring matters for criminal prosecution.

The 2017 Act is not retrospective; OFSI's civil enforcement powers only apply to breaches which have occurred after 1 April 2017.

In order to impose a civil monetary penalty, OFSI must be satisfied on the balance of probabilities that there has been a breach or failure to comply with an obligation imposed by or under financial sanctions legislation, and that the person or corporation in breach knew or had reasonable cause to suspect that they were in breach of the prohibition or had failed to comply with the obligation.

If OFSI can estimate the value of the funds involved in the breach, the maximum penalty is the greater of £1,000,000 or 50% of the estimated value. In all other cases, the maximum penalty is £1,000,000.

Why OFSI hasn't yet used its civil powers

OFSI has been empowered to impose heavy fines for breaches of sanctions at its discretion for the past 18 months, so why has it been so reluctant to exercise these powers?

An initial clue lies in a blog written by the Head of Enforcement and Engagement for OFSI on 29 March 2018:

'I think that the best enforcement is 100% compliance – that is, everyone has properly assessed their risks, taken sensible steps to manage them and, consequently, doesn't break the law. That can only happen if people

understand how financial sanctions work – what your risk is and how the law applies to you'.

In other words, and consistent with the statement of intent in the 2015 Summer Budget, OFSI's compliance and enforcement strategy has to date been concerned with ensuring that financial sanctions are 'properly understood' and 'implemented' as a necessary precursor to 'enforcement' (an overall policy summarised by OFSI as: 'promote, enable, respond [and] change'). To the extent that 'preventative education', promoting a culture of compliance, and 'capacity development' are successful, resort to 'hard' enforcement powers may be less necessary.

Second, and perhaps most significantly, the 2017 Act is not retrospective; OFSI's civil enforcement powers only apply to breaches which have occurred after 1 April 2017. The fact that penalties have not been imposed to date should therefore not be taken as an indication of the overall health of sanctions compliance in the UK. OFSI investigations into some reports of suspected breaches are ongoing and the regime's 'youth' together with OFSI's initial compliance strategy has resulted in a measure of early restraint that cannot be assumed to persist indefinitely. OFSI has made plain in its guidance that it is in the process of 'learning'. Part of OFSI's own learning has been the 'mock' application of its civil enforcement powers to pre-April 2017 breaches reported to it: telling a reporting company that had it been able to apply a monetary penalty to the breach, it would have done so and specifying an amount of such a penalty. OFSI will become more confident in its enforcement function as it 'matures'. In the interim, it is biding its time until it receives reports of sufficiently serious breaches post-dating the April 2017 start date that are appropriate for disposal by way of civil monetary penalties.

A third (and related) reason why OFSI has not yet imposed penalties is that it has thus far preferred to exercise its soft powers. Those powers include: (1) contacting persons and explaining OFSI's view that the action may breach sanctions; (2) issuing correspondence requiring details of how a party proposes to improve their compliance practices in the future; or (3) issuing warnings or cautions. Of course, OFSI's willingness to exercise those 'soft' powers will invariably depend on a number of factors. An indication of 'circumstances in which [OFSI] may consider it appropriate' to impose civil monetary penalties may be gleaned from OFSI's statutory guidance, most recently the Monetary Penalties for Breaches of Financial Sanctions Guidance issued in May 2018.

In the May 2018 guidance, OFSI sets out its case assessment and penalty decision strategy (see box).

OFSI's guidance is due to be revised in April 2019 and there are indications that the existing approach of restraint and reluctant punishment may change.

The guidance stresses the need for a 'proportionate' and 'fair' assessment of every case and states that penalties will only be imposed in cases classified as 'serious' or 'most serious'. OFSI emphasises in its guidance (at 4.4) that the imposition of a penalty is permissive and not mandatory: 'If the penalty threshold is reached, we may impose a penalty. We have discretion not to do so.'

The May 2018 guidance identifies a non-exhaustive list of factors that OFSI will take into account when deciding whether to impose penalties. The following factors will generally tend in favour of penalties:

1. funds or economic resources are made available to a designated person;
2. intentionally and knowingly circumventing sanctions and/or facilitating a breach by others;
3. high-value breaches;
4. calculated and deliberate breaches and possibly also where there is evidence of neglect or a failure to take reasonable care (other, less serious, factors OFSI will consider are whether there has been a systems and control failure, an incorrect legal interpretation, a lack of awareness of one's responsibilities or simply a mistake);
5. serious harm to the sanctions regime's objectives;
6. actual or expected knowledge of and the extent of ways of complying with the sanctions;
7. repeated, persistent or extended breaches.

(See also box on following page.)

Monetary penalties are on the horizon

OFSI's guidance is due to be revised in April 2019 and there are indications that the existing approach of restraint and reluctant punishment may change. Certainly, the fact that OFSI has not exercised its hard powers to date should not be taken as an indication that it will not do so in future. In fact, the OFSI 2018 annual report expressly states that penalties are on the horizon, though it suggests that they will remain

OFSI Monetary Penalties for Breaches of Financial Sanctions Guidance (May 2018)

Discretion not to impose a penalty

4.21 To ensure fair treatment of all on whom we impose a penalty, we will normally follow the above process in each case. However, we reserve the right not to impose a penalty in certain circumstances. These may vary, but will generally include the following:

- imposing the penalty would have no meaningful effect – for example, the value of the penalty is so low it would neither deter offending nor provide restitution for the wrongdoing;
- imposing the penalty would be perverse – for example, the tests for a penalty are met but there is clear evidence that the offence arose from improper coercion;
- it is not in the public interest to impose a penalty.

OFSI Monetary Penalties for Breaches of Financial Sanctions Guidance (May 2018)

Seriousness factors

- 'We are likely to treat a case that directly and openly involves a designated person more seriously than one that is a breach of financial sanctions but does not make funds or economic resources available to a designated person and openly involves a designated person more seriously than one that is a breach of financial sanctions but does not make funds or economic resources available to a designated person' (3.16)
- 'OFSI takes circumvention very seriously because it attacks the integrity of the financial system and damages public confidence in the foreign policy and national security objectives that the sanctions regimes support. We will normally impose a monetary penalty if the case is not prosecuted criminally.' (3.17)
- 'A high-value breach is generally more likely to result in enforcement action.' (3.18)
- 'Calculated and deliberate flouting of sanctions' (3.18), likewise OFSI will consider 'whether the breach seems to be deliberate; whether there is evidence of neglect or a failure to take reasonable care; whether there has been a systems and control failure or an incorrect legal interpretation; whether the person seems unaware of their responsibilities; or whether there has simply been a mistake' (3.24)
- 'The greater the risk of harm to the regime's objectives, the more seriously we are likely to regard a case' (3.19)
- 'The level of actual or expected knowledge and the extent of relevant ways of complying' will be taken into account (3.20)
- 'Repeated, persistent or extended breaches' are more likely to result in 'more serious action' being taken by OFSI (3.28)

the exception rather than the rule: 'It is likely that OFSI will impose monetary penalties in 2018-19. We will continue to consider the full range of potential action in every case. The majority of cases, as now, will be resolved by enforcement activity short of a penalty.'

This prediction is supported by the number of suspected breaches which have been reported to OFSI: in 2016, £75 million worth of breaches was reported, while in 2017 the total was £1.4 billion. Some of these cases are still under investigation. Between the coming into force of the 2017 Act and the publication of its 2018 annual report, OFSI received reports of 103 contraventions. As the number of reports increases, so too does the likelihood that OFSI will find cases which cross its penalty threshold, and that it will broaden its 'fair and proportionate' focus on soft compliance to encompass stronger punitive measures.

That trend would echo the approach taken by OFAC, where monetary penalties have been used extensively and for many years. In 2017, OFAC imposed fines of $119 million on companies found to have breached US financial and trade sanctions, including companies based in the EU.

DPAs

In addition to imposing civil penalties, OFSI now has another tool since the 2017 Act brought financial sanctions into the scope of deferred prosecution agreements for the first time. Rather than pursuing criminal prosecutions, those who are found to be in serious breach of UK sanctions may be permitted to enter into a DPA. OFSI has not issued separate guidance on DPAs; the DPA Code of Practice adopted by the Crown Prosecution Service and the Serious Fraud Office will apply, together with the Code for Crown Prosecutors and the Joint Prosecution Guidance on Corporate Prosecutions. Factors such as self-reporting and restorative measures would likely be prerequisites to a prosecutor offering a DPA, which is in keeping with OFSI's emphasis to date on compliance and monitoring rather than the use of punitive measures.

As OFSI matures and the number of breaches reported to it increases so will the number of cases which could appropriately be resolved by way of a DPA. That said, the Rolls-Royce, Tesco and Skansen Interiors cases show that obtaining the offer of, and successfully negotiating and obtaining judicial approval for, DPAs can be complex and by no means a given outcome in a seemingly appropriate case. We anticipate that DPAs will remain relatively limited in sanctions cases and that OFSI will look first to use its monetary penalties powers. As such, OFSI's approach will have similarities to HMRC's use of its compound penalties scheme in export control cases.

Concluding observations

Much of the commentary on the potential impact of Brexit upon the UK's financial sanctions landscape has focused upon the substance of the UK's future sanctions regimes rather than their enforcement. The government has reaffirmed the UK's commitment to the application of EU sanctions after Brexit; for example, at the Munich Security Conference in February 2018, Prime Minister Theresa May stated: 'We will look to carry over all EU sanctions at the time of our departure. And we will all be stronger if the UK and EU have the means to co-operate on sanctions now and potentially to develop them together in the future'. The new Sanctions and Anti-Money Laundering Act 2018 enables that transition. Beyond the immediate aftermath it remains to be seen precisely what the UK's sanctions post-Brexit landscape will look like. The potential penalties that can be imposed in the UK for sanctions breaches are already greater than in many European states. What is likely is that the UK's sanctions enforcement will increase in frequency and severity as OFSI embraces its new powers.

Rachel Barnes, Patrick Hill and Genevieve Woods are barristers at 3 Raymond Buildings in London where they each practise in financial, corporate and regulatory crime.

www.3rblaw.com

An update on US and EU Russia sanctions and the energy market

Sanctions imposed on Russia by the United States and European Union present considerable challenges to many businesses – the oil and gas sector being amongst the most significantly affected. Recent divergence of law and approach only adds to the complexity, writes Brett Hillis.

In 2014, the US and the European Union introduced sanctions against Russia in response to Russian activity in Crimea and Eastern Ukraine. Initially, the US and EU regimes developed in step, and while there were always differences as to the targets of sanctions and detailed differences of interpretation, the broad approach of the regimes was aligned. More recently, the approaches of the two have diverged, with US sanctions becoming more stringent and EU sanctions staying the same. The divergence has been particularly important to the energy market, given that some of the new US sanctions specifically target Russian energy businesses, and Russia is the EU's largest supplier of energy, particularly natural gas,[1] and a major competitor of the US in oil and gas markets.

This article reviews the relevant US and EU sanctions regimes concerning Russia (and to a relevant extent Ukraine/Crimea) and considers potential future developments.

US SANCTIONS AGAINST RUSSIA

Overview of legal framework

The US framework consists of executive orders and statutes, alongside regulations of the US Treasury Department, Office of Foreign Assets Control ('OFAC'), as set out in the diagram, over, 'US legal framework'.

Under the US regime, the ability of a 'US Person' to trade energy products with Russian or Russian-connected persons (or be concerned in this activity) is affected by whether the counterparty is blocked as a Specially Designated National ('SDN') or is included in the Sectoral Sanctions Identification ('SSI') List.

For the purposes of these sanctions, a US Person is defined as:

[A]ny United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.[2]

Thus, the US sanctions apply to US citizens, US incorporated companies, green card holders and any person in the territory of the United States.

The US regime bars US Persons from dealing with SDNs. In addition, US Persons are prohibited from providing new debt or equity above a specified maturity to persons included in the SSI List.

In 2017, the US Congress passed the Countering America's Adversaries Through Sanctions Act ('CAATSA'), codifying sanctions previously imposed by executive orders thereby limiting the ability of President Trump unilaterally to lift sanctions. In addition, CAATSA put in place secondary sanctions, under which non-US Persons engaging in 'significant transactions' with SDNs risk themselves becoming subject to sanctions. As will be explained below, the passing of CAATSA has resulted in a divergence between the initially similar US and EU approaches.

Effect on the energy market

The US sanctions target both US and non-US Persons, although the restrictions for each type of person differ. A US Person is subject to the Russia/Ukraine-related prohibitions regardless of location. This includes (i) employees of EU companies holding US citizenship and (ii) EU branch offices of US companies. Subsidiaries of US Persons incorporated outside the US are not themselves US Persons.

SDNs

As mentioned, primary sanctions apply to the assets of SDNs, and prohibit US

Persons from dealing with these SDNs.

The prohibition on dealing with SDNs is very wide and, in broad terms, covers any economic activity. Property, and interests in property, of SDNs belonging to or controlled by US Persons, or in the US, must be blocked or frozen and reported to OFAC. Pursuant to executive orders 13660, 13661, 13662, and 13685, OFAC has designated a number of entities in and connected to Ukraine and Russia as SDNs.

Secondary sanctions apply to non-US Persons who engage in or facilitate 'significant transactions' with SDNs. The term 'significant transaction' is intentionally left undefined, thereby giving OFAC more discretion and to discourage non-US companies from doing business with sanctioned entities.

Non-US Persons can also violate US sanctions if they: (1) 'cause' US Persons to engage in violations (such as causing a US financial institution to violate sanctions by processing US dollar payments relating to sanctioned transactions); or (2) allow their US personnel to facilitate, approve, assist, or otherwise participate in prohibited transactions. It should be noted that non-US Persons (such as non-US banks and customers) themselves may be caught by enforcement actions when processing US dollar payments relating to sanctioned transactions.

Since CAATSA was passed, OFAC has listed approximately 40 prominent Russian companies and officials as SDNs under CAATSA. OFAC recently notified Congress, on 19 December 2018, of its intention to terminate its sanctions in relation to UC Rusal plc, En+ Group plc and JSC EuroSubEnergo within 30 days in light of a number of changes and commitments that these entities have agreed to. Unless Congress attempts to oppose this termination on the basis that it considers these changes and commitments inadequate and in accordance with certain provisions under CAATSA within this 30-day window, these entities will be delisted in January 2019.

SSI List

The SSI List includes major companies in key sectors of the Russian economy targeted by the four sectoral sanctions directives: (i) financial services, (ii) defence and related materials, and (iii) the energy sector of Russia. The SSI List therefore applies to specific persons and entities operating within these sectors.

This is different from the SDN List, as the latter prohibits nearly all activities and is broader in scope. A US Person can trade with a Russian entity on the SSI List, provided it does not breach the specific provisions of the Directives. The SSI List does not apply to non-US Persons.

In particular, directives 1,[3] 2,[4] and 4[5] are relevant. The directives are subject to the '50 Percent Rule', which states that 'any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons is itself considered to be a blocked person'[6]

Since CAATSA was passed, OFAC has listed approximately 40 prominent Russian companies and officials as SDNs under it.

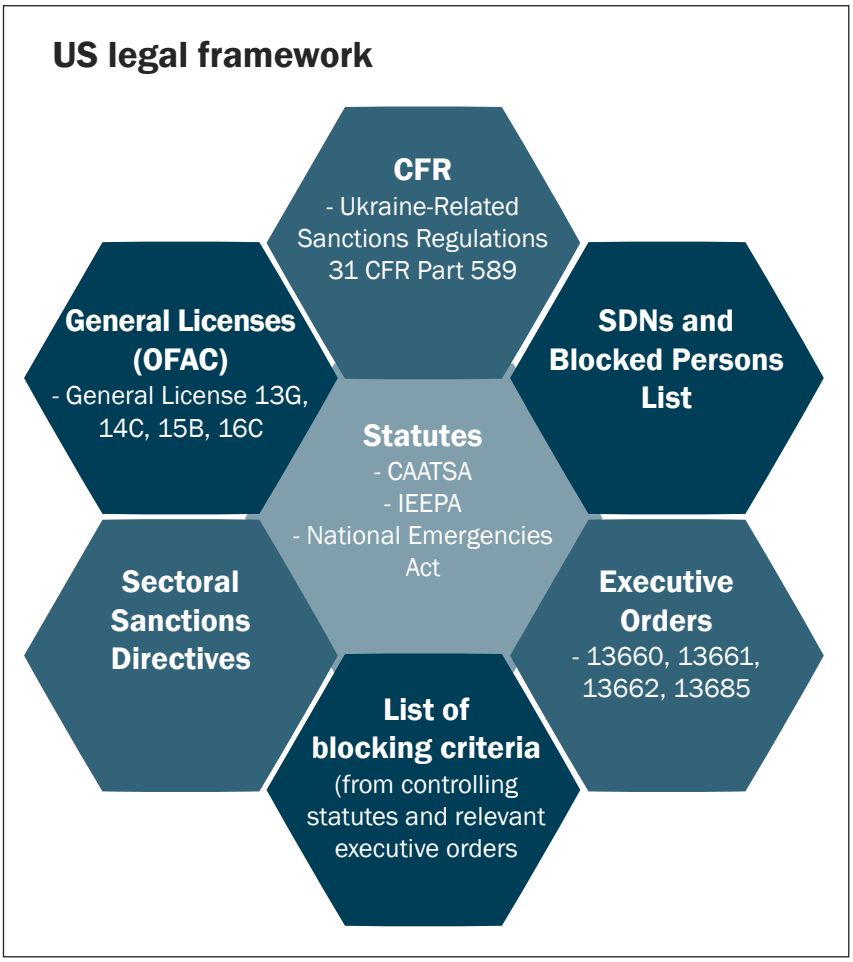
Directive 1 targets equity and debt finance aspects of transactions, prohibiting US Persons from transacting in, providing financing for, or otherwise dealing in new equity or new debt with maturities beyond a set threshold.

For new debt or new equity issued on or after 12 September 2014 and before 28 November 2017, the term is 30 days maturity.

For new debt or new equity issued on or after 28 November 2017, the prohibition extends to all transactions in, provision of financing for, and other dealings in, new debt or longer than 14 days maturity or new equity of persons listed pursuant to Directive 1 (i.e., major banks in the Russian financial services sector).

Directive 2 applies to the Russian energy sector by prohibiting transactions in, providing financing for, and other dealings in new debt with a maturity of longer than 60 days with persons identified on the SSI List under Directive 2. This tightens payment obligations.

For example, US Persons dealing with SSI-listed companies under



Directive 2, e.g., Rosneft, would have to request payment within 60 days of delivery.

Directive 4 further expands on the sanctions targeting the Russian energy sector. Originally, it prohibited US Persons from doing any of the following:

'(1) the provision, exportation, or reexportation, directly or indirectly, of goods, services (except for financial services), or technology;
(2) in support of exploration or production for deepwater [underwater activities at depths of more than 500 feet], Arctic offshore, or shale projects (the Covered Projects);
(3) that have the potential to produce oil in the Russian Federation, or in maritime areas claimed by the Russian Federation and extending from its territory; and that involve any person identified on the SSI List under Directive 4, including that person's property, or its interests in property.'

Since 31 October 2017, OFAC widened the scope of Directive 4 by prohibiting US Persons from providing goods, services and technology for new projects anywhere in the world, in addition to Covered Projects in Russia, where a person subject to Directive 4 has 33% ownership or more.

Crimea
Since 2014, US primary sanctions imposed on Crimea (the 'Crimea embargo') prohibit US Persons from engaging in nearly all commercial transactions with Crimea (under Executive Order 13685).

The Crimea embargo applies to new investment; importation into the US of goods, services or technology from Crimea; exporting or re-exporting, directly or indirectly, any goods, services or technology to Crimea; facilitating any transaction with Crimea; and donating humanitarian goods to Crimea. It also adds new entities to the SDN list.

Special Russian crude oil project (US)
There are also US secondary sanctions targeting non-US Persons engaging in crude oil projects in Russia. The US President must impose sanctions on any person that 'knowingly makes a significant investment' in such a 'special Russian crude oil project' unless this would against national security interests. A 'special Russian crude oil project' is defined as:

'[A] Project intended to extract crude oil from (i) the exclusive economic zone of the Russian Federation in waters more than 500 feet deep; (ii) Russian Arctic offshore locations; or (iii) shale formations located in the Russian Federation.'

Similar to 'significant transaction', 'significant investment' is intentionally undefined to enhance OFAC's discretion and to discourage non-US companies from doing business with sanctioned entities. As part of its discretion when deciding whether to list a person, OFAC considers various issues, such as the size, frequency and nature of the transactions in question.

The approach of the EU sanctions regime against Russia is broadly similar to the US approach pre-CAATSA.

Russian energy export pipeline sector (US)
Investment by non-US Persons in Russian energy pipelines is likely to be affected, since CAATSA authorises the imposition of secondary sanctions on those that knowingly:

- supply Russia with goods, services or technology, or
- invest USD 1 million or more (or USD 5 million or more over a 12-month period).

To be caught by the sanctions, the supply or investment must directly and significantly boost Russia's ability to construct energy export pipelines (such as the Nord Stream 2 natural gas pipeline from Russia to Germany).

These sanctions must be imposed 'in coordination with the allies of the US'. However, these authorities have not been exercised and their use is likely to depend on the developing political stance towards Russia.

Reliefs on sanctions
The US framework contains some reliefs for US Persons when dealing with certain named SDNs. OFAC issued general licences permitting US Persons to wind down their dealings with certain named SDNs, and for the divestment or transfer of debt, equity, or other holdings in SDNs.

Additionally, activities undertaken by US Persons that are covered by general licences do not constitute 'significant transactions' for the purposes of secondary sanctions. As mentioned, non-US Persons violate US sanctions if they: (1) 'cause' US Persons to engage in violations (such as causing a US financial institution to process payments in sanctioned transactions); or (2) allowing their US personnel to participate in prohibited transactions.

It is advisable for non-US Persons to refrain from dealings that attract high risks of secondary sanctions and blocking sanctions.

EU SANCTIONS AGAINST RUSSIA

Overview of legal framework
As mentioned above, the approach of the EU sanctions regime against Russia is broadly similar to the US approach pre-CAATSA. This approach has been renewed each year and has not changed significantly since 2014-2015.

The main regulation consists of sectoral sanctions pursuant to Council Regulation (EU) No. 833/2014 ('the Regulation'), and is supported by asset freezes of certain individuals (i.e., people involved in Russian activities in Crimea and Ukraine) and entities involved in the misappropriation of public property and human rights violations in Ukraine.[7] In particular:

- Article 2 prohibits transactions relating to dual-use goods and technology;
- Article 3 restricts the supply of

technologies for the Russian oil industry;
- Article 5 prohibits the provision of new debt or equity to certain entities beyond 30 days maturity, as well as related securities.

Effect on the energy market (EU)
Article 2 of the Regulation prohibits:

- the sale, supply, transfer or export, directly or indirectly, of dual-use goods and technology to, or for use in Russia if the items are, or may be, intended for military use;[8] and
- the provision of technical and financial assistance, brokering and other services to entities specifically identified in annex IV of the Regulation (i.e., companies involved in the weapons and arms trade).

Article 3 requires exporters to seek prior authorisation for the sale, supply, transfer or export, directly or indirectly, of technologies for the oil industry to any person, entity or body in any country, if such equipment or technology is for use in Russia (including its Exclusive Economic Zone and Continental Shelf).

'Technologies' include oil/gas lines and drill pipelines, pumps, platforms, etc. as listed in annex II of the Regulation, and pertain to deep-water oil exploration and production, Arctic oil exploration and production, or shale oil projects in Russia.

Like Article 2, authorisation under **Article 3** would not be possible if the competent authorities have reasonable grounds to believe that the activity is for the aforementioned prohibited uses (i.e., deep-water oil exploration, etc.). Under both articles, authorisation may be granted if the export relates to an obligation arising from a contract or an agreement concluded before 1 August 2014, or ancillary contracts necessary for execution of such a contract.[9]

Article 5 targets transactions relating to transferable securities and money-market instruments. Articles 5(2)(b) and (c) specifically prohibit direct and indirect dealings with transferable securities and money-making instruments with a maturity exceeding 30 days, issued after 12 September 2014 by, amongst others, a legal person, entity or body established outside the EU listed in annex VI (which, at the time of writing, are Rosneft, Transfet and Gazprom Neft).

Article 5(3) prohibits directly or indirectly making or being part of any arrangement to make new loans or credit, with a maturity exceeding 30 days to certain publicly owned Russian financial institutions. Those covered by the prohibition include: (i) major financial institutions (established in Russia with over 50% public ownership or control) as listed in annex III, and (ii) a legal person, entity or body established outside the EU whose proprietary rights are directly or indirectly owned for more than 50% by an entity listed in Annex III. This prohibition does not apply to loans or credit that have a specific and documented objective to (i) provide financing for non-prohibited imports or exports of goods and non-financial services between the EU and any non-EU state or (ii) provide emergency funding to meet solvency and liquidity criteria for legal persons established in the EU.

At the time of writing, the entities identified in annex III are: Sberbank, VTB Bank, Gazprombank, Vnesheconombank, and Rosselkhozbank

To ensure uniform implementation by national authorities and parties concerned, the EU Commission has published a guidance note ('the Guidance' on the implementation of certain provisions of the Regulation.[10] It is interesting to note in the context of trading energy, the Guidance has clarified that 'derivatives used for hedging purposes in the energy market are not covered' under article 5 prohibitions.

The EU Blocking Statute – Council Regulation (EC) No. 2271/96

The EU Blocking Statute shields EU companies from the extra-territorial application of certain foreign sanctions laws and foreign court judgments based on those foreign sanctions laws. Currently, the only 'blocked' US sanctions laws under the EU Blocking Statute relate to trade and investment embargoes imposed by the US on Cuba, Iran and Libya.

Future US and EU changes

Any further US change to its Russian sanctions regime will be influenced not only by any future Russian actions but also by political developments within the Trump administration and the US Congress. The complex political scenario means that it is difficult to predict what will happen. That said, given the current Democrat House of Representatives, the US stance will likely not be rolled back.

In contrast, EU sanctions have simply been rolled over, and in economic terms, did not change in response to the Salisbury Novichok poisoning. A likely explanation for the limited change in the EU position is its Member States' differing stances towards Russia and that any changes to the sanctions regime will require agreement from all 28 Member States. For example, in September 2018, France backed the UK's calls for an EU sanctions regime for chemical weapons use in response to the poisoning whilst Italy stated that it was not their intention to do so. Barring any substantial changes due to the European Parliament elections in 2019 or any future Russian actions, it is not foreseeable that the EU would roll back or intensify its approach to the sanctions regime against Russia.

Links and notes

1 https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies/supplier-countries
2 31 CFR § 589.312
3 As amended on 29 September 2017
4 As amended on 29 September 2017
5 As amended on 31 October 2017
6 Department of the Treasury, "Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked", 13 August 2014
7 Council Regulation (EU) No 692/2014 (as amended); Council Regulation (EU) No 269/2014 (as amended); and Council Regulation (EU) No 208/2014 (as amended)
8 Annex I of Regulation (EC) No. 428/2009
9 Amending Regulation No. 960/2014
10 As amended by Regulation No. 1290/2014
11 As amended by Regulation No. 1290/2014
12 Commission Notice C(2015) 6477 of 25 September 2015

Brett Hillis is a partner in the London office of international law firm Reed Smith where he focuses on the energy sector.

bhillis@reedsmith.com

Promoting biosecurity through export controls

While emerging technologies in the life sciences can offer potentially huge benefits for mankind, in the hands of the malicious actor they may become a dangerous weapon. This dual-use nature of developing sciences, writes Dr. Betty Lee, creates a challenge for which export control regimes need be prepared.

Emerging technologies in the life sciences – such as synthetic and systems biology, nanotechnology, and research into genomes – promise great benefits to mankind through new synthetic drugs, gene editing and precision medicine, as well as in areas such as nutrition, agriculture and the development of biofuels.

This is research that thrives in an interdisciplinary and international environment, where information sharing is encouraged: doing so enables others to advance the sphere of knowledge and the commensurate rewards for humanity. But it is also intrinsically dual-use in nature and the risk of misuse – for example, by rogue states or non-state actors looking to develop new forms of WMD – is high.

Defining biosecurity

While every organisation defines biosecurity differently, the definition coined by the US National Academy of Sciences certainly covers the bases:

'Security against the inadvertent, inappropriate, or intentional malicious or malevolent use of potentially dangerous biological agents or biotechnology, including the development, production, stockpiling, or use of biological weapons as well as outbreaks of newly emergent and epidemic disease.'[1]

In an area where scientific advance is so rapid, technology is developing faster than it can be regulated.

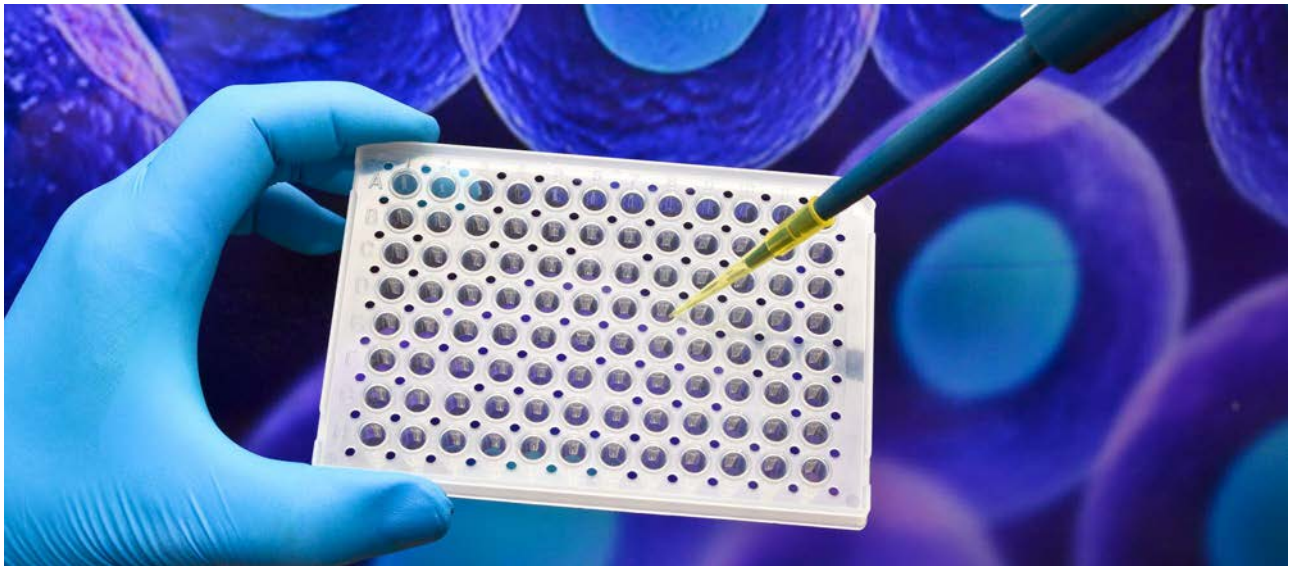
The World Health Organization has defined the goal of biosecurity as being 'to prevent, control and/or manage risks to life and health as appropriate to the particular biosecurity sector.'[2]

But while the tools provided by the various export control regimes provide important mitigation of biosecurity risks, there are reasons why they cannot be wholly relied upon to do so. Not least of these is that in an area where scientific advance is so rapid, technology is developing faster than it can be regulated.

Another reason is that threat and benefit need to be carefully evaluated. This 'double-edged sword' is amply illustrated by the example of the conundrum presented in 2012, as to whether to publish results of H5N1 avian influenza transmissibility in mammals.

The results of the experiments into the creation of modified, more transmissible viruses, appeared to enhance the chances of a pandemic, owing to either a lab accident or intentional release by terrorists.[3] On the other hand, they also represented a scientific advance of great value to the community.

Such studies highlight the dilemma attendant on the publication of the results of dual-use research of concern ('DURC'). The results of research in the life sciences are usually shared in publications to advance knowledge and potential benefits for that branch of science. However, in the case of some sensitive studies which have dual-use potential, the research benefits must be weighed against the risk of proliferation threat.



Synthetic truths

The case of the DNA synthesiser – a piece of equipment that is critical to the pursuit of research in the field of synthetic biology – illustrates how biosecurity is enhanced by the use both of export controls and industry best practice.

Recently, the synthesiser has been added to both the Australia Group ('AG') list, and the US Commerce Control List ('CCL'), administered by the Bureau of Industry and Security ('BIS') within the Department of Commerce.

The equipment is controlled where it meets the specification of being 'partly or entirely automated and able to generate continuous nucleic acids greater than 1.5 kilobases in length with error rates less than 5% in a single run'.[4]

Such equipment poses a challenge for biosecurity, as the technology makes it convenient and easy to synthesise a toxin or viral gene. DNA sequences synthesised by a DNA synthesiser can be combined to obtain the genome of a controlled pathogen.

As the equipment is still expensive, researchers rely on DNA providers to synthesise their genes of interest. Commercial DNA synthesiser companies belong to consortia that voluntarily conduct screening of sequences and customers. A voluntary security practice in the form of sequence screening was adopted by the International Gene Synthesis Consortium ('IGSC').[5] These companies apply a common protocol for screening DNA orders and customers while promoting the benefits of gene synthesis. There are currently 12 gene synthesis companies in the IGSC and they represent 80% of the gene synthesis business worldwide.

Once a project is identified as DURC [dual-use research of concern] , it calls for a careful evaluation of the benefit of the research to public health.

IGSC aims to promote the beneficial application of gene synthesis technology while safeguarding biosecurity.

In a report of the 2016 Symposium on Export Control of Emerging Biotechnologies in Monterey, California, USA, participants emphasised that the current DNA synthesisers permit the synthesis of small RNA viruses[6] and that next generation synthesisers with the ability to stitch together these segments such as assemblers, should be carefully evaluated to see whether a list-based approach of control would be useful to prevent misuse of the technology. (Unfortunately, there was no consensus.)

Research of concern

There are, helpfully a number of resources available to those involved in life science research that can assist in the decision-making around project funding and publication.

In the US, the Government Policy for Oversight of Life Sciences Dual Use Research of Concern came into force in 2012.[7] This outlines steps that should be taken to determine whether projects fall under the definition of DURC, to assess the risks and benefits on a regular basis, and to develop risk-mitigation plans for federal agencies that conduct or fund life sciences research.

The DURC policy covers 15 specific agents and toxins for seven defined categories of experiments that are already on the federal Select Agent Program, established under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. This policy aims to limit the scope to prevent the over-control of legitimate research that does not pose much of a risk and to limit the associated burden on research institutions.

Once a project is identified as DURC, it calls for a careful evaluation of the benefit of the research to public health. In addition, grant reviewers need to consider the biosafety and biosecurity conditions under which the research will be conducted, and risk mitigations – e.g., the potential risk that the knowledge may be misused by terrorists. As mentioned above, an example of DURC would be research to enhance the transmissibility of H5N1 viruses.

However, the subjective evaluation

of experiments that are commonly agreed to be DURC exposes the dilemma as to whether it addresses the DURC issue at all. Further, the policy is limited to federally funded research and doesn't apply to private or industry sponsored research.

Group think?

On the export control front, the key multilateral regime relevant to life sciences is the Australia Group, founded in the 1985 in response to the use of chemical weapons in the Iran-Iraq war.

The AG is an informal group of 42 countries and the European Union, whose shared objective is to ensure that the export of chemicals, biological agents, dual-use chemical and biological equipment and technologies does not contribute to chemical and biological warfare. Its role is to coordinate the national export control policies of its members to promote non-proliferation of both chemical and biological weapons, and its scope includes pathogens and biotech-related equipment.[8]

Member states are obliged to harmonise their export controls to the AG Control List as a vital means of ensuring that legitimate trade in chemicals, biological agents, and related equipment can continue.[9] The AG meets on an annual basis in Paris to discuss ways of deterring proliferators from acquiring essential materials or technology for CBW (chemical and biological warfare) programmes and assisting each country's national export control laws.

In the US, the Bureau of Industry and Security of the Department of Commerce is the regulatory agency that oversees export controls of dual-use technology and items. Its mission is to protect the security of the United States, which includes its national security, cyber, economic, and homeland security.

Because of its inherent risks, dual-use research in the life sciences requires some oversight by government and funding agencies. In the case of biotechnology, equipment used for manufacturing medicines and food production such as fermenters, freeze drying equipment and filtration systems can be used for nefarious purposes. Export controls also apply to intangible technologies for the development, production, or use of items on the AG control list or the CCL.

Links and notes

1 https://www.nap.edu/catalog/11567/globalization-biosecurity-and-the-future-of-the-life-sciences Globalization, Biosecurity, and the Future of the Life Sciences (2006)

2 http://www.who.int/foodsafety/fs_management/No_01_Biosecurity_Mar10_en.pdf INFOSAN Information Note No. 1/2010 – Biosecurity)

3 Uhlenhaut C1, Burger R, Schaade L. EMBO Rep. 2013

4 https://www.bis.doc.gov/index.php/forms-documents/regulations-docs/2333-ccl2-10-24-18/file

5 https://genesynthesisconsortium.org/

6 https://www.nonproliferation.org/wp-content/uploads/2017/04/op26-findings-from-the-2016-symposium-on-export-control-of-emerging-biotechnologies.pdf Fairchild

7 http://oba.od.nih.gov/oba/biosecurity/PDF/United_States_Government_Policy_for_Oversight_of_DURC_FINAL_version_032812.pdf)

8 Shaw, R. 'Export controls and the life sciences: controversy or opportunity?'EMBO Rep. 2016 Apr; 17(4): 474–480 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4818776/

9 http://www.australiagroup.net/en/introduction.html

10 https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators

Regulators normally publish lists of 'red flag indicators' to help industries identify suspicious purchase enquiries designed to circumvent export controls and divert dual-use goods to WMD.[10]

However, the latest breakthroughs in biotechnology are not reflected on the AG or CCL lists in a timely way, because the pace of progress is too rapid. It takes several years of proposals and or discussion before the AG can reach a consensus to either add, change or delete items from the list, while scientific researchers have an incentive to publish their discoveries and share the knowledge with the rest of the world as soon as possible in order to apply for grants from government entities.

Because of its inherent risks, dual-use research in the life sciences requires some oversight by government and funding agencies.

A case in point is that of the gene-editing tool, CRISPR-Cas9, which promises to be useful in the eradication of infectious diseases, the generation of new biofuels and the production of disease-resistant plants and animals. But this dual-use technology can also be used for nefarious purposes to increase the pathogenicity or transmissibility of microorganisms or insect vectors.

However, numerous scientific articles about the tool's ability to manipulate mammalian genes have already been published in peer review journals. As the information about the technology is publicly available, it would be pointless for the AG to attempt its control.

In conclusion

Export control is a non-proliferation tool to balance legitimate commercial use and also prevent nefarious uses. Countries with similar strategic trade/export controls regulations will benefit from identical control lists as they will be able to use the legal tool to prevent proliferators from acquiring technology or equipment to create bioweapons.

Export control is one checkpoint to promote biosecurity and the challenge is to be aware of or prepared for emerging technology that may make some controlled items or technology obsolete. As research proceeds at a rapid pace, the control lists need to be regularly updated to be useful as a non-proliferation checkpoint.

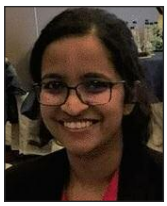
Meanwhile, best practice and outreach within and toward the relevant communities remains an essential component of biosecurity.

The opinion of the author does not represent the official view of the US Department of Commerce.

Dr. Lee works as a Licensing Officer in the Chemical and Biological Controls Division, Office of Non-Proliferation and Treaty Compliance, Bureau of Industry and Security, US Department of Commerce in Washington, DC.

betty.lee@bis.doc.gov

Sanctions in close-up – application and practice in India

Sanctions in India are known as 'Prohibitions' and they typically conform with UN Security Council resolutions. Ameeta Verma Duggal and Aditi Warrier provide a deep dive into the Indian sanctions regime and insight into the country's approach to controlling exports.

For several years now, India has had provisions regulating trade, financial transactions, and the entry of sanctioned individuals into Indian territory. These are focused on the country's commitment to a policy of not assisting, encouraging or inducing any country to manufacture weapons of mass destruction ('WMD') and to prevent non-State actors and terrorists from acquiring WMD and their means of delivery. Such regulations are targeted towards maintenance of national security, public order and fulfilment of obligations under the Charter of the United Nations for the maintenance of international peace and security, and take the form of sanctions or export control measures.

The word 'sanction' finds no mention in the laws of India and is instead referred to as 'Prohibitions'. India imposes Prohibitions, classifiable as country-specific, product-specific and organisation, group or individual-specific. The Prohibitions imposed by India conform to the obligations cast on the Member States of the United Nations, pursuant to various United Nations Security Council resolutions ('UNSCR'). The most frequently applied Prohibitions in India are with respect to trade in arms, nuclear material and nuclear-related materials, prohibited financial assistance, and entry of sanctioned individuals through India.

India is a member of the Missile Technology Control Regime, Wassenaar Arrangement and the Australia Group, besides being an adherent country to the Nuclear Suppliers Group. Accordingly, India's export control laws are compliant with these multilateral export control regimes.

The word 'sanction' finds no mention in the laws of India and is instead referred to as 'Prohibitions'.

India mandates exports of all strategic goods, services and technology being subject to specific authorisations depending on end use and end-user. Such items are listed in the Special Chemicals, Organism, Materials, Equipment and Technologies ('SCOMET') List, which includes nuclear materials and nuclear-related materials, equipment and technology; munitions and chemical and biological weapons.

Regulatory framework for imposition of Prohibitions

The most effective way of implementing Prohibitions has been to curb trade with the target country. In India, exports and imports of goods, services or technology are generally 'free' except when prohibited or regulated by the central government.

The Prohibitions are implemented through the Directorate General Foreign Trade in the Ministry of Commerce & Industry ('DGFT'), being the nodal authority regulating India's foreign trade policy ('FTP'), formulated pursuant to the Foreign Trade (Regulation and Development) Act, 1992 ('FTDR'). The FTDR – which regulates these Prohibitions and the exports, transfers, re-transfers, transit, transshipment of and brokering in SCOMET items – in turn, incorporates by reference the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005 ('WMD Act'). The WMD Act was enacted pursuant to UNSCR 1540 (2004), which had necessitated the provison of integrated legal measures to exercise controls over the export of materials, equipment and technologies capable of use in WMD and their means of delivery and to prohibit unlawful activities in relation thereto.

While the overall regulation of Prohibitions and export controls vests with DGFT, exports of nuclear materials and nuclear-related materials, equipment and technology are authorised by the Department of Atomic Energy, and exports under the Munitions List are authorised by the Department of Defence Production, Ministry of Defence.

The UNSCRs that govern non-proliferation also provide for combating the financing of proliferation of WMD. These include

- general resolutions, such as UNSCR 1373 (2001) and 1540 (2004);
- country-specific resolutions, such as UNSCR 1718 (2006) and 2231 (2015) against DPRK and Iran, respectively; and
- organisation-, group- or individual-specific resolutions, such as UNSCR 2199 (2015) with respect to organisations and individuals such as the Islamic State in Iraq and the Levant ('ISIL'), Al Nusrah Front ('ANF') and others associated with Al Qaida.

Violation of financial sanctions warrants action under the Prevention of Money-laundering Act, 2002 ('PMLA') and the Unlawful Activities (Prevention) Act, 1967 ('UAPA'). The implementation of these sanctions involves inter-departmental actions, particularly between the Ministry of External Affairs, Department of Economic Affairs, Ministry of Home Affairs, Financial Intelligence Unit India ('FIU-Ind'), Reserve Bank of Inida ('RBI'), Securities and Exchange Board of India ('SEBI') and the Insurance Regulatory Development Authority ('IRDA') (collectively, 'Regulators').

The Ministry of Home Affairs undertakes regular threat assessments regarding terrorism and its financing and the Ministry of External Affairs keeps the Regulators updated on requirements under UNSCRs.

Prohibitions under the FTP

In compliance with sanctions imposed under UNSCRs, the extant Prohibitions extend to the following:

1. Direct or indirect import and export to/from Iran;
2. Direct or indirect import and export from/to the Democratic People's Republic of Korea ('DPRK');
3. Import and export of arms and related material from/to Iraq;
4. Import of charcoal from Somalia;
5. Trade with ISIL (also known as 'Daesh'), Al Nusrah Front and other individuals, groups, undertakings and entities associated with Al Qaida.

Direct or indirect import and export from/to DPRK of items, materials, equipment, goods and technology are prohibited.

Prohibition on trade with Iran

Direct or indirect import/export from/to Iran of any item, material, equipment, goods and technology mentioned in the following documents is permitted subject to the provisions contained in annex-B to UNSCR 2231 (2015):

(i) Items listed in INFCIRC/254/Rev.9/Part 1 and INFCIRC/254/Rev.7/Part 2 (International Atomic Energy Agency, 'IAEA' documents) as updated by the IAEA from time to time;
(ii) Items listed in S/2006/263 (UNSC document) as updated by the UNSC from time to time.

These documents list the items, materials, equipment, goods and technology which could contribute to Iran's enrichment-, reprocessing-, or heavy water-related activities, or to development of nuclear weapon delivery systems.

Prohibitions on trade with the DPRK

Direct or indirect import and export from/to DPRK of items, materials, equipment, goods and technology are prohibited. Specifically, exports to DPRK are subject to the UNSCRs on DPRK, namely: 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2094 (2013), 2270 (2016), 2231 (2016), 2356 (2017), 2371 (2017) and 2375 (2017) and 2397 (2017). This list is subject to periodic revision.

Prohibition on export

(A) Direct or indirect supply, sale, transfer or export of:

(i) Any battle tanks, armoured combat vehicles, large calibre artillery systems, combat aircraft, attack helicopters, warships, missiles or missile systems as defined for the purpose of the United Nations Register on Conventional Arms, or related materiel including spare parts;
(ii) All arms and related materiel, including small arms and light weapons and their related materiel;
(iii) All items, materials, equipment, goods and technology as set out in the UNSC and IAEA documents, namely:
  a) S/2006/853;
  b) S/2006/853/Corr.1;
  c) Part B of S/2009/364;
  d) Annex III of UNSCR 2094 (2013);
  e) S/2016/1069;
  f) Annex A to INFCIRC/254/Rev.12/Part 1 (IAEA document);
  g) Annex to INFCIRC/254/Rev.9/Part 2 (IAEA document);
  h) S/2014/253;
  i) S/2016/308;
  j) Annex III of UNSCR 2321 (2016); and
  k) other items, materials, equipment, goods and technology, as determined by the central government, which could contribute to DPRK's nuclear-related, ballistic missile-related or other WMD-related programmes;
(iv) Luxury goods, including, but not limited to, the items specified in annex IV of UNSCR 2094 (2013), annex IV of UNSCR 2270 (2016) and annex IV of UNSCR 2321 (2016);
(v) Items as determined by the central government (except food or medicine) that could directly contribute to the development of

operational capabilities of the DPRK's armed forces subject to exemptions and procedures set out in paragraph 8 (a) and (b) of UNSCR 2270 (2016).

Prohibition on import

(B) The direct or indirect procurement or import from the DPRK, of items, whether or not originating in the DPRK, covered in sub-paragraphs (A)(i), (A)(ii), (A)(iii) and (A)(v) above.

Sectoral prohibitions (export)

(C) Direct or indirect supply, sale, transfer or export of:

(i) New helicopters and new or used vessels, except as approved in advance by the UNSC Committee set up pursuant to paragraph 12 of UNSCR 1718 (2006) ('the Committee') on a case-by-case basis;
(ii) Aviation fuel, including aviation gasoline, naphtha-type jet fuel, kerosene-type jet fuel, and kerosene-type rocket fuel subject to exemptions and procedures set out in paragraph 31 of UNSCR 2270 (2016) and paragraph 20 of UNSCR of 2321 (2016);
(iii) Condensates and natural gas liquids;
(iv) Refined petroleum products subject to exemptions and procedures set out in paragraph 5 of UNSCR 2397 (2017);
(v) Crude oil subject to exemptions and procedures set out in paragraph 4 of UNSCR 2397 (2017);
(vi) All industrial machinery, transportation vehicles, and iron, steel and other metals subject to exemptions and procedures set out in paragraph 7 of UNSCR 2397 (2017);

Sectoral prohibitions (import)

(D) Direct or indirect import of:

(i) Coal, iron and iron ore subject to exemptions and procedures set out in paragraph 8 of UNSCR 2371 (2017);
(ii) Gold, titanium ore, vanadium ore, and rare earth minerals;
(iii) Copper, nickel, silver and zinc;
(iv) Statues, unless the Committee approves on a case-by-case basis in advance;
(v) Seafood (including fish, crustaceans, molluscs, and other aquatic invertebrates in all forms) subject to exemptions and procedures set out in paragraph 9 of UNSCR 2371 (2017) and paragraph 6 of UNSCR 2397 (2017);
(vi) Lead and lead ore subject to exemptions and procedures set out in paragraph 10 of UNSCR 2371 (2017);
(vii) Textiles (including but not limited to fabrics and partially or fully completed apparel products) subject to exemptions and procedures set out in paragraph 16 of UNSCR 2375 (2017);
(viii) Food and agricultural products, machinery, earth and stone including magnesite and magnesia, wood and vessels subject to exemptions and procedures set out in paragraph 6 of UNSCR 2397 (2017).

Prohibition of trade with Iraq

Import/export of arms and related material from/to Iraq. However, export of arms and related material to the government of Iraq is permitted subject to a specific 'No Objection Certificate' from the Department of Defence Production.

Prohibitions on trade with Somalia

In accordance with UNSCR 2036 (2012), the FTP prohibits direct or indirect import of charcoal from Somalia, irrespective of whether or not such charcoal has originated in Somalia. Accordingly, importers of charcoal in India are required to submit an express declaration to customs that the consignment has not originated in Somalia.

Importers of charcoal in India are required to submit an express declaration to customs that the consignment has not originated in Somalia.

Prohibitions in other laws

India maintains a list of terrorist groups, individuals and entities under the UAPA ('the Designated List'), which includes organisations listed in the Schedule to the UN Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order 2007 made under the United Nations (Security Council) Act 1947. The Designated List is updated regularly by the Ministry of External Affairs subject to the other UN sanctions and communicated to the Regulators. Further, requests received from other countries pursuant to UNSCR 1373 (2001) are considered by the Ministry of External Affairs and the Designated List is accordingly updated.

The UAPA empowers the government to

- freeze, seize or attach funds and other financial assets or economic resources held by or on behalf of or at the direction of the individuals or entities that are covered under the Designated List or any other person engaged in or suspected to be engaged in terrorism;
- prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities in the Designated List or any other person engaged in or suspected to be engaged in terrorism; and
- prevent the entry into or through India of individuals in the Designated List or any other person engaged in or suspected to be engaged in terrorism.

With respect to funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies and so on, the Regulators forward the Designated List to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies. All financial transactions are counter-checked against the Designated List and suspicious transactions are required to be reported to FIU-Ind. The Ministry of

Prohibitions on trade with terrorist groups

In compliance with the UNSCR 2199 (2015), trade in oil and refined oil products, modular refineries and related materials, besides items of cultural (including antiquities), scientific and religious importance are specifically prohibited with the Islamic State in Iraq and the Levant ('ISIL'), Al Nusrah Front ('ANF') and other individuals, groups, undertakings and entities associated, directly or indirectly, with Al Qaida.

Home Affairs also forwards the Designated List of individuals to the immigration authorities and security agencies with a request to prevent the entry into or transit through India. Compliance against the Designated List is reported to the Ministry of Home Affairs by various agencies involved, which forwards the same to the Ministry of External Affairs for onward reporting to the United Nations.

India is also a member of the Financial Action Task Force ('FATF'), the independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of WMD. The FATF recommendations are recognised as the global anti-money laundering and counter-terrorist financing standard. The RBI takes into consideration the advisory issued by FATF to protect the international financial system from ongoing money laundering and terrorist financing risks emanating particularly from DPRK, Iran, Afghanistan, Iraq, Syria and Yemen, while noting that such advisories do not preclude the regulated entities from legitimate trade and business transactions with these countries. The RBI has aligned its instructions to the objectives of FATF and prohibited an Indian party from making direct investment in an overseas entity (set up or acquired abroad directly as a joint venture/wholly owned subsidiary or indirectly as a stepdown subsidiary) located in countries that are identified as non-cooperative by FATF or as otherwise notified by the RBI.

Enforcement of Prohibitions

The Prohibitions are enforced through multiple authorities, including DGFT, Customs, Department of Revenue Intelligence, Enforcement Directorate and so on depending on the nature of offence. Some of the broad penalties that may get attracted to cases involving violations of Prohibitions are shown in the table, right.

USA sanctions and India

India has always been reluctant to implement unilateral sanctions imposed by other countries. Most recently, India has had to deal with the sanctions imposed by the United States under the Countering America's Adversaries Through Sanctions Act,

S No	Act	Penalty
1.	FTDR	i. Suspension or cancellation of the Importer Exporter Code. ii. Inclusion in the Denied Entity List. iii. Penalty of not less than ten thousand rupees and not more than five times the value, whichever is more. iv. Confiscation.
2.	WMD Act	i. In case of unlawful manufacture, acquisition, possession, development or transport of a weapon of mass destruction or their delivery system, imprisonment for minimum 5 years extendable to life, with fine. ii. In the event of export of any material, equipment or technology knowing that it is intended to be used in the design of weapons of mass destruction: (a) first offence, minimum imprisonment of 6 months extendable upto 5 years with fine. (b) subsequent offences, minimum imprisonment of 1 year extendable upto 7 years with fine.
3.	Atomic Energy Act, 1962	Imprisonment for a term, which may extend to five years, or with fine, or both.
4.	Customs Act, 1962	i. Confiscation. ii. Penalty not exceeding three times the value of the goods as declared by the exporter or the value as determined under the Customs Act, whichever is higher. iii. Imprisonment for a term which may extend to seven years and with fine. iv. In the case of preparation for export of prohibited goods, imprisonment for a term which may extend to three years, or with fine, or with both.
5.	PMLA	i. Rigorous imprisonment for a term not less than three years but which may extend to seven years and fine. ii. Seize, attach, freeze or confiscate property involved in the money-laundering. iii. Arrest any person believed reasonably to be guilty.
6.	UAPA	i. Punishment for unlawful activities – imprisonment for a term which may extend to seven years, and fine. ii. Penalty for being member of an unlawful association – imprisonment for a term which may extend to two years, and fine. iii. Penalty for being member of an unlawful association and committing any act resulting in loss of human life – punishable with death or imprisonment for life, and fine. iv. Penalty for dealing with funds of an unlawful association – issuance of a prohibitory order and if the person continues to act in prohibition of the order, imprisonment for a term which may extend to three years, or with fine or with both and an additional fee. v. Punishment for conspiracy – imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and fine. vi. Punishment for being member of a terrorist organisation - imprisonment for a term which may extend to imprisonment for life, and fine. vii. Punishment for holding proceeds of terrorism – imprisonment for a term which may extend to imprisonment for life, and fine. viii. Punishment for contravention of the Explosives Act, or the Explosive Substances Act, or the Inflammable Substances Act, or the Arms Act, with intent to aid any terrorist or terrorist organisation – imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and fine.
7.	Arms Act	i. Punishment for bringing into, or taking out of India, any arm or ammunition prohibited by the Central Government for import or export – imprisonment for a term which shall not be less than three years but which may extend to seven years and fine. ii. Punishment for bringing into or taking out of India any arm or ammunition without licence for import and export of arms – imprisonment for a term which shall not be less than one year but which may extend to three years and fine.

2017 ('CAATSA') on Iran and Russia.

As *WorldECR* readers will know, following the US withdrawal from the Joint Comprehensive Plan of Action in May 2018, the US imposed sanctions against Iran effective November 2018. However, eight countries, including India, were specifically exempted by grant of a 'waiver' for a period of six months (unless expressly extended), allowing them to continue buying Iranian oil. India and Iran, have shared historical ties and Iran is India's major oil supplier. India has also made substantial investment of $500 million to develop Iran's Chabahar Port as a transit hub for Afghanistan, Central Asia and the International North-South Transport Corridor. Besides, India is also developing two gas fields in and around Iran. It is, therefore, not easy for India to disengage itself from Iran. To overcome the transactional difficulties posed by the US sanctions, India has signed a bilateral agreement with the National Iranian Oil Company to settle oil trades in Indian currency (which is not freely traded on international markets) through an Indian government-owned bank. India has also exempted these rupee payments from taxes. The rupee payments will be used by Iran to pay for imports from India, invest in Indian businesses, pay for Iranian missions and students in India, and so on.

India also countered the CAATSA sanctions against Russia and signed a defence deal for the purchase of the Russian-built S-400 Triumf or the SA-21 Growler, a long-range surface-to-air missile system. India gives primacy to its individual diplomatic relations, including with Iran, Russia and the United States, which surpasses the unilateral sanctions imposed by any individual country. India is a strategic partner for the US, having recently been conferred Srategic Trade Authorisation-1 status, which saw the US ease controls on high-tech exports to India. It is believed that US will not endanger its relations with India over the Russia defence deal.

Conclusion

With ever-growing concern over proliferation of weapons of mass destruction threatening international peace and security, coupled with India's membership of the multilateral export control regimes, India is becoming aggressive in its enforcement of Prohibitions and export controls. It has an established and robust legislative framework to counter proliferation of WMD and terrorism. Now the authorities are focused on enforcing the same through inter-departmental cooperation in investigations and joint enforcements. The lead is being taken by the intelligence agencies and customs. Shipments and movement of individuals from or to sanctioned countries are under intense scrutiny. India's commitment to a safe and secure world is steadfast.

Ameeta Verma Duggal is the founder partner of DGS Associates. Aditi Warrier is an associate with the firm.

www.dgsassociates.in

Out now: Chinese language version of guide to investing in US critical industries

'Successful investing in the United States is possible, but you must prepare.' So says Reid Whitten, editor of *The CFIUS Book*, a new guide on how to navigate an investment or acquisition in sensitive industries or companies in the US, which is now available from *WorldECR* in a Chinese language edition.

What is CFIUS and why does it matter?

CFIUS is the Committee on Foreign Investment in the United States. It is a Committee of nine US agencies that is authorised to review any transaction that may result in foreign control of a US company.

CFIUS reviews investment in the US to determine whether it may affect national security, then clears it, proposes steps to mitigate national security risk, or prohibits or unwinds the deal. Recently, attention has focused sharply on FIRRMA , The Foreign Investment Risk Review Modernization Act, signed into law on 13 August 2018. This expanded the scope of CFIUS jurisdiction beyond transactions in which a foreign company takes control of a US business.

CFIUS has the power to unwind a deal – so if you're planning an investment or acquisition in a US company which could be considered impacting US national security, it's important that you're well prepared.

One step at a time

The CFIUS Book provides straightforward examples, illustrated charts, and highlighted key points on the best approaches to success for a US investment.

The CFIUS Team at law firm Sheppard Mullin Richter & Hampton maps out the paths to and through the CFIUS process, from the decision to submit a notification, through tips and traps along the way, to the CFIUS safe harbour, including the most recent updates under the Foreign Investment Risk Review Modernization Act, or FIRRMA.

The CFIUS Book also includes chapters from Sheppard Mullin's specialists in National Security and NISPOM as well as Team Telecom and the particular requirements for space-related investments.

Contents

The CFIUS Book introduces the Committee, explains its history and the powers it wields, answering questions including

- What is CFIUS?
- What is FIRRMA?
- Why CFIUS matters to you

Readers are taken through the process, with helpful, valuable guidance as you

- Analyse whether you need to file a CFIUS notice
- Gather your information, draft and submit your notice
- Receive CFIUS review and response

Additional chapters tackle areas such as parallel foreign investment reviews and the expansion of CFIUS interest into privacy and data security.

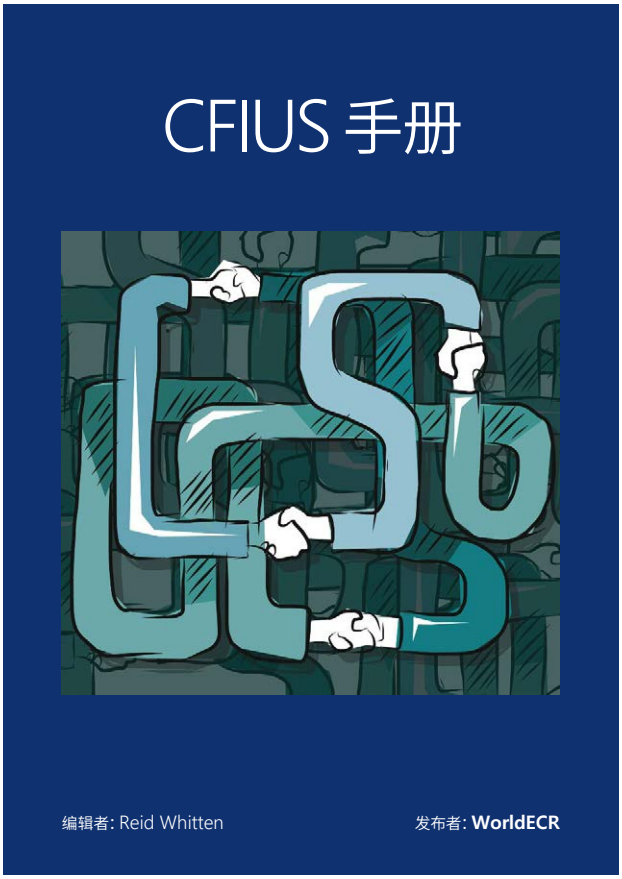
Who needs this book?

Outside the United States:

- Private equity companies looking to invest in the United States
- Strategic investors considering US acquisitions
- Persons interested in US infrastructure assets such as pipelines, ports, airports, power grids, or related assets
- Potential investors in US companies storing significant amounts of personal data such as healthcare, financial, network platforms, and data and telecoms companies
- Investors in US sectors such as defence, telecoms and satellite, government contracting, chemical or biological, or nuclear
- Banks or investment banks involved in any such investment
- Insurance companies, including representation and warranties insurers, involved in any such investment
- Attorneys or consultants representing any such investment

In the United States

- Private equity companies selling a US portfolio company to a foreign buyer
- US companies that may be sold in industries like defence, telecoms and satellite, government contracting, chemical or biological, or nuclear
- Persons selling infrastructure assets such as pipelines, ports, airports, power grids, or related assets
- Banks or investment banks involved in any such transaction
- Potential target US companies storing significant amounts of personal data such as healthcare, financial, network platforms, and data and telecom service companies
- Insurance companies (including representations and warranties insurers) involved in any of such transaction
- Attorneys or consultants representing any such transaction



The CFIUS Book is edited by Reid Whitten and published by WorldECR. It costs £120 a copy (104 pages).

To purchase a Chinese language copy, please contact **mark.cusick@worldecr.com**

To purchase an English language copy, please visit **www.worldecr.com/books**

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Rachel Barnes, Patrick Hill and Genevieve Woods, 3 Raymond Buildings
www.3rblaw.com

Ameeta Verma Duggal and Aditi Warrier, DGS Associates
www.dgsassociates.in

Brett Hillis, Reed Smith
www.reedsmith.com

Dr. Betty Lee, Bureau of Industry and Security, US Department of Commerce
www.bis.doc.gov

WorldECR Editorial Board

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0076]

Correspondence address: D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road, London N1 7GU, England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road, London, UK

ISSUE 76. FEBRUARY 2019
www.WorldECR.com