WorldECR

A British 'Blue Lantern' – would it work? 9

Establishing an effective export compliance organisation 21

Turkish delight: sanctions, tariffs, and the new normal 23

US Congress threatens more sanctions against the Russian government 24

US ramps up sanctions activities against North Korea in 2018 27

Transit and the transport service providers – victims or facilitators? 29

US controls: What every healthcare and life sciences compliance officer needs to know 35

ISSUE 72. SEPTEMBER 2018
www.WorldECR.com

Brexit: Would 'no deal' be a big deal for UK exporters?

With the saga of Britain's withdrawal from the European Union continuing to confound and confuse public and 'experts' alike, at least some clarity has emerged in the field of export controls in the form of recently published guidance from the UK's Export Control Joint Unit ('ECJU') and Department for International Trade ('DIT') – on how exporting controlled goods would be affected if the UK leaves the EU without a Brexit deal, a scenario which the UK prime minister, Theresa May, has described as being, 'not the end of the world'.

The technical notice covers:

- How export licensing requirements for different groups of items would change;
- What the UK government would do to simplify licensing;
- Where exporters of military and dual-use items, civilian firearms, and other goods can find relevant information.

It says that in the event of there being no deal,

- The movement of dual-use items from the UK to the EU would require an export licence. This is not currently the case and these movements would, therefore, need to be licensed in the same way as for non-EU destinations.
- Extant export licences issued in the UK would no longer be valid for exporting dual-use items from EU Member States. A new licence, issued by an EU Member State, would be required.

The ECJU guidance covers how export licensing requirements for different groups of items would change.

- Extant export licences issued by the 27 EU countries would no longer be valid for exporting dual-use items from the UK. A new licence, issued by the UK, would be required.

It offers some consolation, however, in the form of reassurance that the European Court of Justice would seek to minimise additional administrative burdens 'by making available an Open General Export Licence for export to the EU, which exporters could easily register to use through our existing online platform.'

This, explained a government spokesperson to *WorldECR,* would 'permit the export of specified items to specified countries, following an online registration, which removes the need for exporters to apply for individual licences, as long as the exporters can meet the terms and conditions set out in the licence.'

Anthony Rapa, a partner at the law firm Kirkland & Ellis, shared with *WorldECR* his observations about the prospect in view, noting that while the overall impact of Brexit on UK export controls may turn out to be limited, 'there is a greater chance of divergence between the UK and EU regimes in a "no deal" scenario.'

Extant export licences issued in the UK would no longer be valid for exporting dual-use items from EU Member States.

He said that Brexit could affect UK export controls in three key areas:

1. the composition of the UK dual-use control list;
2. potential licensing requirements for exports of UK export-controlled items to the EU; and
3. the contours of UK jurisdiction over dual-use items.

According to Rapa, 'The impact of a "no deal" Brexit may be most keenly felt with respect to the composition of the UK dual-use list. As a threshold issue, the UK, as a participant in the Wassenaar Arrangement and other multilateral export control regimes, will maintain a baseline dual-use control list that is identical to the EU list, regardless of whether there is a negotiated or "no deal" Brexit. However, the extent to which the UK controls additional dual-use items not currently subject to any multilateral controls could depend on the type of Brexit that comes to pass. In a negotiated scenario, the UK could agree to mostly harmonise its control list with the EU's, even while ostensibly retaining the freedom to control additional items (which in fact the UK has now – a tool it uses only sparingly).

'In a "no deal" scenario, however, there would be no constraints at all on the UK's ability to control additional dual-use items. In that case, the UK could drift towards a US-type position by which it would control additional items pursuant to (a) UK-centric foreign policy concerns (e.g., imposing export controls targeting Russia following a Skripal-type incident, imposing controls on countries the UK considers to be sponsors of terrorism, etc.), and/or (b) the UK's interest in controlling sensitive/emerging technologies (a path on which the US is about to embark).

'With regard to export licensing, the outcome similarly could depend on whether there is a negotiated or "no deal" Brexit, although in practice there may not be much difference for exporters.

'Currently, the UK imposes a licensing requirement for exports of dual-use items out of the

continues

UK, except for most exports to the EU and countries eligible under EU General Export Authorisation No. EU001 (i.e., the US, Norway, etc.). Following Brexit, exports from the UK to the EU would be just that – exports – and potentially subject to a licensing requirement. In a negotiated scenario, it is possible there would not be any licensing requirement. With a "no deal" Brexit, however, as the ECO guidance has made clear, there would be a licensing requirement, although the UK government would issue an OGEL authorising exports to the EU (subject to a registration requirement). Thus, it seems that even in the worst case scenario – where there is a licensing requirement for exports to the EU – there would be an OGEL authorising such exports, and the only real burden for exporters would be to register in order to use the OGEL. Interestingly, I suppose it remains to be seen what other countries would be eligible under such an OGEL. Presumably it would also include the countries covered by EU General Export Authorisation No. EU001.

'Finally, with regard to UK export jurisdiction, it is possible that in a "no deal" scenario, the UK could eventually take an expansive view of its export control jurisdiction. The EU export control regime, like most others in the world, is strictly territorially based – that is, the EU Dual-Use Regulation regulates exports out of the territory of the EU. Presumably the UK will follow this course. However, the US regulates not only exports out of the US, but all exports around the world of (a) US-origin items, (b) non-US items that incorporate more than a *de minimis* level of controlled US content, and (c) certain non-US items that are the direct product of certain US technology. Eventually, in particular if there is a "no deal" Brexit, the UK could adopt a similarly extraterritorial approach to dual-use controls, although I am not aware of any proposal to do so in the near or medium term.'

The technical notice is one of a number of notices published by Department for Exiting the European Union to advise industry sectors on what happens in the event of a 'no deal', and while the notice emphasises that a no-deal outcome is 'unlikely', Dr. Liam Fox, the Secretary of State for International Trade, has said publicly that he believes no deal is more likely than not.

The ECJU's technical notice can be found here:

https://www.gov.uk/government/publications/exporting-controlled-goods-if-theres-no-brexit-deal

US sanctions Russia over use of chemical weapons

On 24 August, the US Department of State announced new sanctions against Russia, effective from 27 August. The new restrictions on exports, targeting arms sales and foreign assistance, follow the Trump administration's finding that Russia was responsible for the chemical poisoning of the Skripals which took place in Salisbury, UK, in March this year.

The sanctions, authorised under the Chemical and Biological Weapons Control and Elimination Act 1991 for the duration of one year, focus chiefly on government bodies and state-owned enterprises rather than a wider class of recipients. The sanctions involve the termination of foreign military sales and an export licensing ban on defence articles; the termination of foreign military financing; the denial of US government credit or other financial assistance; and a licensing policy of denial for sensitive goods and technology, such as dual-use items, to the Russian government or state enterprises.

The continuing export of certain dual-use items will be unaffected, although new licence requests will be considered on a case-by-case basis. Space flight activities, cooperation over government space projects, commercial aviation safety and urgent humanitarian assistance will be exempt. Under the act, unless President Trump certifies to Congress within three months that Russia is no longer using chemical or biological weapons in violation of international law, further sanctions will be imposed. These could include a ban on all exports, other than food and agricultural commodities; restrictions on the import of Russian goods; a ban on state-owned air carriers travelling to or from the US; US opposition to the provision of financial or technical assistance by international financial institutions to Russia; or a downgrading of diplomatic relations between the two countries.

Congress is currently considering two bills that may ratchet up financial and trade sanctions against Russia for its alleged hacking of the 2016 US presidential election: The Defending American Security from Kremlin Aggression Act of 2018 and The Defending Elections from Threats by Establishing Redlines Act of 2018 (see Barbara Linney's article this issue).

During his recent visit to the US, new UK Foreign Secretary Jeremy Hunt called upon the EU to follow the US's lead in imposing sanctions in response to the Salisbury attack. It is not clear whether this will happen, as a unanimous decision by all 28 States would be needed to take action against Russia, with Italy and Greece reluctant to press for sanctions against Russia in the past.

The notice in the Federal Register can be found here:

https://www.govinfo.gov/content/pkg/FR-2018-08-27/pdf/2018-18503.pdf

WorldECR welcomes your news. Email tom.blass@worldecr.com

US reimposes Iran sanctions and EU reactivates Blocking Regulation

The US has re-imposed certain sanctions on Iran lifted under the 2016 Joint Comprehensive Plan of Action ('JCPOA'). President Trump issued an executive order re-imposing these sanctions from 7 August following the expiry of the first 90-day 'wind-down' period after his 8 May announcement that the US was pulling out of the nuclear deal. Other sanctions will be re-imposed following the expiry of the second 180-day 'wind-down' period on 4 November.

Sanctions re-imposed from 7 August include those concerning:

- The purchase or acquisition of US dollar banknotes by the Iranian government;
- Iran's trade in gold or precious metals;

New US sanctions from 7 August have prompted the EU to bring its updated Blocking Regulation into force.

- The sale, supply or transfer (whether direct or indirect) to or from Iran of materials such as graphite, raw or semi-finished metals, including aluminium and steel, coal and software, or integrating industrial processes;
- 'significant' transactions involving the purchase or sale of Iranian rials, or maintenance of 'significant' funds or accounts outside Iran denominated in rials;
- The purchase, subscription to or facilitation of the issuance of Iranian sovereign debt;
- Iran's automotive sector.

Other 'wind-down' authorisations previously issued by OFAC concerning the importation of carpets or food from Iran, as well as certain licences for the export or re-export of commercial passenger aircraft, parts and services, also expired on 7 August.

Sanctions re-imposed from 5 November include those concerning:

- Iranian port operators and energy, shipping, and shipbuilding sectors;
- Transactions involving petroleum or petroleum products;
- Transactions by foreign financial institutions with the Central Bank of Iran.

OFAC has issued FAQs on the Iran sanctions. These include guidance on when payments from Iranian parties can be received after the wind-down periods.

EU response

The EU has responded by bringing its updated Blocking Regulation into force (7 August). This means that no judgment or requirements from an authority outside the EU concerning the re-imposition of US sanctions on Iran will be recognised, and EU persons should not comply with any requirements or prohibitions unless that would seriously damage their interests or those of the European Union.

Damages caused by the US sanctions, including legal costs, can be 'clawed back' by the affected party.

The EU has issued a guidance note to assist commercial operators with the adoption of the update to the Blocking Regulation.

Commission Delegated Regulation (EU) 2018/1100 can be found here:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2018.199.01.0001.01.ENG&toc=OJ:L:2018:199I:TOC

For the Guidance Note on the Blocking Regulation, see:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.CI.2018.277.01.0004.01.ENG&tForoc=OJ:C:2018:277I:TOC

For the Executive Order, see:
https://www.whitehouse.gov/presidential-actions/executive-order-reimposing-certain-sanctions-respect-iran/

For OFAC's FAQs, see:
https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180806.aspx

US, Russia and others impeding law on 'killer robots'

The governments of the United States, Russia and others are impeding progress on a law which would place controls on the development of so-called 'autonomous' weapons, says a pressure group called Stop Killer Robots.

Following the recent meeting on lethal autonomous weapons systems at the UN Convention on Conventional Weapons ('CCW'), the group (an umbrella organisation whose members include Human Rights Watch and the International Committee for Robot Arms Control) said that while the 88 states participating substantially agreed on the need to retain 'some form of human control over weapons systems and the use of force,' they failed to agree on how best to meet that objective.

It said that most states concurred that negotiations should begin next year on a new treaty to prevent the development and use of lethal autonomous weapons systems, with some calling for a pre-emptive ban treaty, and that Austria, Brazil and Chile 'recommended a new CCW mandate "to negotiate a legally-binding instrument to ensure meaningful human control over the critical functions" of weapons systems.'

But, the group said, a handful of nations (Australia, Israel, Russia, South Korea and the United States) are opposed to any 'new treaty, political declaration or any other new measures to address the dangers posed by these weapons,' and as a result, the meeting concluded 'without having taken concrete steps beyond exploring options for further work'.

Export controls, ICPs and good practice

A 2-day training programme, with Strong & Herd in association with WorldECR

Award-winning Export Controls Consultancy **Strong & Herd**, in association with **WorldECR**, the journal of export controls and sanctions, is delighted to present this two-day, in-depth training on export controls and creating an Internal Compliance Plan which is practical, fit for purpose, and tailored to your company's specific needs.

While eminently suitable for those new to export controls, established professionals will find it a stimulating refresher – and a rare opportunity to share ideas.

The course will cover:

The Basics

- An introduction to export controls – looking at the UK export control system in global perspective
- Military Goods and Dual-Use goods – how do they differ in law? How do I distinguish between them?
- Who, in my company, is responsible for compliance?
- How is the transfer of intangible technology controlled and why?
- Record-keeping and technical information

The Anatomy of Export Controls – an introduction to

- Licensing
- End-users, end-user statements and undertakings
- Catch-all
- Sanctions

Export controls in the United Kingdom

- The Export Control Joint Unit (ECJU) – its role and function
- Licensing applications – getting started with SPIRE
- Knowing your OIELS from your OGELs: distinguishing between types of licence and their application requirements

Outcomes and benefits of attending

Attendees of this intensive, two-day training can look forward to leaving with greater confidence that they understand, and can apply within their own organisations, key concepts and requirements of export control compliance, and generate a checklist of best practice requirements relevant to their own company needs.

All attendees will receive a certificate of attendance.

Preparing for BREXIT

In the light of the UK's intended departure from the European Union, it is imperative for EU and UK companies to understand:

- New licensing requirements for UK exports to the EU and vice versa
- Implications of Brexit for controlled goods supply chains and intra-company transfers
- Potential for further divergence as EU export controls evolve

Export controls and my company

- Where should responsibility for compliance 'sit' in your company?
- Who should be trained in export controls?
- Ensuring export control awareness company-wide
- Record-keeping and preparing for an audit

Case studies presented on the course will explore situations such as

- The classification of goods in different scenarios
- Impact of supplying the same goods to different markets (assessing need for end-use statements or undertakings)
- Sending equipment for repairs or temporarily, for marketing purposes
- How US controls apply in the United Kingdom/European Union

The training will include break-out, industry-specific sessions for representatives from

- Oil/ gas/ energy • Aerospace
- Vehicles • Chemical industries
- Technology – IT/ encryption

- **Export controls, ICPs and good practice, a 2-day training event, will take place on 15-16 November 2018 at The Strand Palace Hotel, 372 Strand, London WC2R 0JJ**
- **Attendance costs £945 (+VAT where appropriate) and includes 2 days of training, breakfast, lunch and morning and afternoon refreshments. Special rates are available for organisations wishing to send 3 or more delegates.**
- **For further information or to reserve your place, email mark.cusick@worldecr.com**

US sanctions 44 Chinese businesses over 'threat to national security'

At the start of August, the US Department of Commerce's Bureau of Industry and Security ('BIS') added 44 Chinese businesses to the Entity List. Those sanctioned included sizable state-owned enterprises and their subsidiaries, as well as those that specialise in high-tech research in the semi-conductor industry. BIS determined that the sanctioned parties have acted 'contrary to the national security or foreign policy interests of the United States'. Some of those listed were determined to be 'involved in the illicit procurement of commodities and technologies for unauthorised military end-use in China.'

Sanctioned entities include state-owned enterprises and high-tech research companies in the semi-conductor industry.

The eight Chinese entities and their 36 subsidiaries are subject to BIS's export licence requirements in addition to the licence requirements imposed by the Export Administration Regulations ('EAR'), and there will be a 'presumption of denial' when considering licences. Licence exceptions will not be available.

The move comes amidst growing concern among US government representatives over the national security risks posed by Chinese state-linked technology companies operating in the US. The Democratic National Committee has reportedly warned its party candidates running in the mid-term November elections not to use devices made by Chinese telecoms companies ZTE Corp or Huawei Technologies because of a perceived security risk.

For the Federal Register of 1 August 2018 see:

https://www.gpo.gov/fdsys/pkg/FR-2018-08-01/pdf/2018-16474.pdf

Saudi Arabia sanctions Canada over call for the release of human rights activists

A tweet by Canadian Foreign Affairs Minister Chrystia Freeland criticising the detention of a Saudi activist has sparked backlash sanctions from Saudi Arabia. The tweet called for the release of Samar Badawi, sister of jailed dissident Raif Badawi, whose wife and children are Canadian citizens. This was followed by a tweet from a Canadian government account calling for the release of 'all other peaceful human rights activists'.

Saudi Arabia's foreign ministry called the statement 'a major, unacceptable affront to the Kingdom's laws and judicial process'. The government imposed the following measures with effect from 6 August:

Canadian Foreign Affairs Minister, Chrystia Freeland's tweet has sparked backlash sanctions from Saudi Arabia.

- The recall of the Saudi Arabian ambassador to Canada and expulsion of the Canadian ambassador;
- The suspension of flights from state-run Saudi Airlines to Toronto;
- The withdrawal of around 12,000 Saudi citizens studying at Canadian universities;
- The freezing of all new trade with Canada (bar oil shipments).

The future of a controversial $12bn arms deal between the two countries is undecided.

The Canadian government's issue of export permits authorising the export of light armoured vehicles to Riyadh, defended by prime minister Justin Trudeau, has received negative coverage in the press over their possible use in the Saudi-led intervention in Yemen.

SocGen confronting $1.4bn sanctions payment

On 3 September, French bank SocGen announced that it has made available $1.4 billion to pay a possible sanctions penalty to US regulators, in the light of an investigation by the Office of Foreign Assets Control of the US Department of the Treasury ('OFAC'), the US Attorney's Office of the Southern District of New York, the New York County District Attorney's Office, the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of New York, and the New York State Department of Financial Services 'regarding certain US dollar transactions processed by Société Générale involving countries that are the subject of US economic sanctions.'

It said that it is entering 'a phase of more active discussions' with the authorities, with a view to reaching a resolution within weeks.

On its website, the bank says that its compliance division 'was reorganised on 1 January, 2018 and directly reports to the Group's General Management, thus becoming an independent division in its own right headed by Edouard-Malo Henry, member of the Group's Management Committee.'

EU maintains sanctions pressure on South Sudan

The EU Council has extended its arms embargo against South Sudan and added two individuals to its sanctions list (10 August).

The sanctions reflect the requirements under UN Security Council resolution 2428 (2018). The EU has had an arms embargo in place against South Sudan since 2011, and the two officials concerned have already been sanctioned by the EU autonomously since February 2018 for involvement in serious human rights violations. The UN sanctions have been adopted 'in view of the ever-deteriorating humanitarian and security situation in South Sudan and considering the lack of commitment by some actors to the ongoing peace process.'

South Sudan has experienced a bloody civil war since 2013, characterised by ongoing violence by both government and armed opposition. Despite a peace agreement brokered in December 2017, millions of people have been displaced and an estimated 300,000 killed.

The EU and UN have stepped up their efforts to find a resolution to the violence in South Sudan as the agreement for the transitional government of national unity (set out in the Agreement on the Resolution of the Conflict in South Sudan ('ARCSS')) expires in 2018. The EU has sanctioned nine individuals under its South Sudan sanctions regime, of which eight are listed by the UN.

Iran sues US over re-imposition of sanctions following JCPOA exit

The International Court of Justice ('ICJ') in the Hague has been hearing evidence in Iran's lawsuit against the US for the re-imposition of sanctions following the US's exit from the Joint Comprehensive Plan of Action ('JCPOA') on 8 May.

In its application, Iran states that through its decision 'to reimpose in full effect and enforce' sanctions against Iran, Iranian companies and its people, the US 'has violated and continues to violate multiple provisions of the 1955 Treaty'. This refers to the Treaty of Amity, Economic Relations and Consular Rights, an infrequently used legal instrument setting out the legal framework for bi-lateral relations between the two countries, entered into when Iran was under the rule of the Shah.

Iran claims the US is in breach of a 1955 treaty between the countries.

The US is urging the ICJ to dismiss the lawsuit, with US State Department legal adviser Jennifer Newstead arguing that Iran's appeal based on the 1955 treaty is a stalling tactic.

'Iran is endeavouring to use the procedures of the Treaty of Amity to enforce rights that it claims under an entirely different (agreement) that specifically excludes judicial remedies,' she said.

US Secretary of State Mike Pompeo has released a statement calling the claim 'meritless' and 'an attempt to interfere with the sovereign rights of the United States to take lawful actions, including re-imposition of sanctions, which are necessary to protect our national security. The proceedings instituted by Iran are a misuse of the Court.'

Iran is arguing that the US sanctions should be suspended until the case is heard in full – which could take years – an outcome which has been robustly rejected by US lawyers. A provisional ruling of the ICJ is expected in around a month.

Although the ICJ is the supreme United Nations court and its decisions are binding, it lacks the means to enforce its judgments and its rulings have been ignored by countries including the US and Iran in the past.

A British 'Blue Lantern' – would it work?

WorldECR considers whether an end-use verification system, along similar lines to the United States' 'Blue Lantern' programme, is appropriate for the United Kingdom and elsewhere.

The UK parliament's Committees on Arms Export Controls ('CAEC') has recommended that the government should consider the end-use monitoring of arms exports.

In its latest report on the export of strategic military and dual-use items for 2016, released on 18 July, the CAEC said that end-use monitoring would 'assist [the government] in making more informed licensing decisions, as well as helping address compliance and enforcement.'

The UK is currently one of the largest arms exporters in the world, supplying military equipment to Saudi Arabia, the Philippines, Israel, the United Arab Emirates ('UAE'), and until recently Venezuela, amongst others. It has secured £3.7bn worth of arms sales to Saudi Arabia since 2015 – controversial at a time when the Saudi-led intervention in Yemen has been accused of 'genocide' against civilians. In 2016 the government faced judicial review proceedings in the High Court brought by Campaign Against the Arms Trade ('CAAT') over the legality of its arms exports to Saudi, which were unsuccessful.

In previous reports the CAEC has recommended the implementation in the UK of a similar programme to the US end-user verification scheme 'Blue Lantern', a comprehensive programme operated by the US State Department's Directorate of Defense Trade Controls ('DDTC').

Under Blue Lantern, US embassy staff make end-user checks in cooperation with the host governments of around 100 countries each year. This kind of arrangement is pretty much unique.

In line with the enforcement of most export control regimes, the UK government has no provision for such systematic end-use monitoring. Instead – as is evident from the CAEC's report – government officials repeatedly emphasise the rigour of assessment during the licence application process. Arms licence applications are considered on a 'case-by-case' basis against the Consolidated EU and National Arms Export Licensing Criteria, one of which is whether there is a 'clear risk' that the items might be 'used for internal repression' or 'in the commission of a serious violation of international humanitarian law'.

The UK is also a signatory to the 2014 Arms Trade Treaty, which obliges member states to monitor arms exports and ensure that arms do not end up in destinations where they can be used for human rights abuses, such as Syria.

System under some fire

But the front-loaded system of checks isn't immune from criticism. The CAEC report notes that in response to several written questions on the use of UK-supplied military equipment by the Israeli Defence Force, the government response was 'We do not collect data on the use of equipment after sale.' According to CAAT, in 2017 the UK issued £221m worth of arms licences for exports to Israel – which has been accused of excessive force in suppressing Palestinian protests – a significant jump from the previous year's figure of £86m.

'The proposal for the UK to have in place some form of stricter end-user verification system than is currently the case, as proposed by the CAEC, is not an easy one for the British government to try to introduce, in our view,' says Brinley Salzmann, director at ADS Group. 'It has to be recognised that the UK is no longer a first world superpower, which can push its weight around, unlike the USA. We have in place (contrary to the constantly-repeated public views of many of the NGOs) a reasonably effective and proportionate export control system, to meet our needs of facilitating responsible exports, whilst seeking to block irresponsible ones.'

It is also likely that UK and foreign intelligence agencies are active in looking for the diversion of goods, particularly where weapons of mass destruction or possible terrorist purposes are concerned.

'Where risks are identified, this is factored into licensing decisions,' says Richard Tauwhare of the London office of law firm from Dechert. 'In practice,

Visitors to a Middle East arms fair examine the merchandise.

therefore … the UK already has a form of end-user verification programme, albeit one that it is not prepared to confirm, and this is probably the most effective means available.'

An overt programme would support the current methods used to detect diversion, he points out, but might be less likely to be able to detect serious cases which would be subject to sophisticated means of deception.

The introduction of a Blue Lantern-style end-use verification programme for UK arms exports also presents practical and legal obstacles. At a time of cutbacks, it is unclear how such a comprehensive enterprise would be resourced, and whether the costs would be passed on to exporters through, for example, charging for licensing. There is also the question of how the verification monitors would access the end-user, which may be in a foreign military or security organisation.

'Making such access a precondition of the export could result in UK companies losing contracts to other suppliers that do not impose such conditions,' says Tauwhare.

A recent report released by the Ministry of Defence in July indicates that the UK defence industry currently contributes over £7bn of exports to GDP each year on average. Another stumbling block is the fundamental legal basis of the UK and indeed the EU, which are both in principle opposed to the extra-territorial reach of their laws, unlike the US.

A recent report released by the Ministry of Defence in July indicates that the UK defence industry currently contributes over £7bn of exports to GDP each year on average.

'It's not really desirable or workable for the UK to set up a post-export monitoring system like the one used by the US,' says Mark Bromley from the Stockholm International Peace Research Institute ('SIPRI'). 'That system is based on the goal of being able to "see through" pretty much every export of controlled items with the goal of ensuring that all re-exports have the prior consent of the US government. That's not something any other country – aside from the United States – is interested in doing. However, it's not clear why something similar to what Germany and Switzerland have done – and which Sweden is in the process of putting in place – would not be workable.'

Alternative approaches

The CAEC heard evidence from Dr Lucie Béraud-Sudreau, a research fellow at the International Institute for Strategic Studies ('IISS'), on end-use monitoring by Switzerland and Germany. These two countries have created post-export controls that apply to certain exports of items that are particularly prone to diversion. Switzerland carried out between three and nine on-site inspections each year between 2014 and 2016, whilst Germany conducted two visits in 2017, to India and the UAE. Both programmes have so far focused on small, light weapons and are circumscribed in their scope.

'The post-shipment controls, introduced in Germany three years ago, is a pilot programme concerning certain military items exported to a few countries outside of the EU and NATO,' says Phillip Haellmigk from Munich-based Haellmigk Lawyers. 'At the moment, the future of the pilot is undecided, but it is my prognosis that it will not be extended to other areas.'

Other alternatives to a comprehensive end-user monitoring programme include 'light touch' methods, such as routine or opportunistic monitoring by UK embassy staff and defence attachés; enhanced due diligence by exporters; enhanced government-to-government assurances for high-risk goods (as already required for some nuclear-related goods) and being prepared to refuse more licences because of the risk of diversion.

Change looks unlikely

After the CAEC's review of arms exports to the Middle East and North Africa in 2011, the UK government announced that it would 'undertake end-use monitoring of controlled military goods, bearing in mind both the practical and resource limitations'. This was not put into effect. Now the matter has been raised by the CAEC again, what is the likelihood of some sort of programme being implemented?

'The government have regularly said they will keep the idea under review,' says Tauwhare. 'But a combination of the costs and practicalities, the lack of evidence that there is a serious problem of the diversion of UK controlled exports, the thoroughness of the risk assessments during the licensing process, and the presumed existence of covert programmes, suggests that they are unlikely to make significant changes in the foreseeable future.'

The CAEC

The Committees on Arms Export Controls ('CAEC') comprises four House of Commons committees: the Defence, Foreign Affairs, International Development and International Trade committees. The key points from the CAEC's report on UK arms exports in 2016 included:

- The possible impact of Brexit on UK arms export controls;
- The recommendation that the government consider tightening the regulation of arms-dealers;
- The request that the government provide information about situations where licensing decisions are made by ministers, rather than by officials;
- The recommendation that the government considers introducing a presumption that certain licences will be denied for exports to countries that have not signed the Arms Trade Treaty or are on the Foreign and Commonwealth Office's list of Human Rights Priority Countries;
- Criticism of the government for presenting data in formats that are very difficult to use – and the misrepresentation of data in relation to prosecutions over export control offences;
- The request that the government review the resources given to HM Revenue & Customs for the enforcement of export controls;
- The expression of dissatisfaction at the government's admission that it carries out no auditing of overseas operations by UK companies in connection with licences, and recommendation that the compliance-audit regime be extended; and
- The recommendation that the government considers whether to start monitoring the final destination of arms exports.

News and alerts

Tank Talk

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

Turkey in a twizzle over defence systems

A report by the Turkish think-tank EDAM explores whether the 'interlinked' issues of the US Congress's reluctance to approve deliveries of the F-35 Lightning II fighter, and Turkey's acquisition of the Russian strategic defensive weapons system S-400 Triumf, could cause irreparable damage to NATO, and transatlantic security. It notes US fears that operating both systems may result in valuable data about the F-35 being transmitted to Russia.

'In our view, Ankara would need to adopt a political and diplomatic strategy that takes fully into account of this inevitable conclusion that the acquisition of the S-400s will have ramifications for the supply and operationalization of the F-35s. Either the US will need to be convinced that the delivery of the F-35s to a country that operates the Russian-made S-400s is not a real threat to the integrity of networkcentric NATO platforms, or that the threat of cyber hacking – or digital espionage – emanating from the S-400s can categorically be eliminated, or Turkey would need to forego the acquisition – or at the very least the operationalization – of the S-400s. At present, there seems to be no real third option for Turkish policy-makers to sidestep these binary and mutually exclusive outcomes.'

http://edam.org.tr/en/is-turkey-sleepwalking-out-of-the-alliance-an-assessment-of-the-f-35-deliveries-and-the-s-400-acquisition/

2020 vision

Nuclear war between the United States and North Korea is unthinkable – isn't it? Earlier this year, Dr Jeffrey Lewis, East Asia Program Director at the Middlebury Institute of International Affairs at Monterey was commissioned to write a novel, exploring the set of mishaps and mis-steps that could lead to such a thing. A flavour of the book (which has been compared to other apocalyptic reads, such as Neville Shute's *On The Beach* can be gleaned from the dust jacket:

'"The skies over the Korean Peninsula on March 21, 2020, were clear and blue." So begins this sobering report on the findings of the Commission on the Nuclear Attacks against the United States, established by law by Congress and President Donald J. Trump to investigate the horrific events of the next three days.

'An independent, bipartisan panel led by nuclear expert Jeffrey Lewis, the commission was charged with finding and reporting the relevant facts, investigating how the nuclear war began, and determining whether our government was adequately prepared for combating a nuclear adversary and safeguarding U.S. citizens.

'Did President Trump and his advisers understand North Korean views about nuclear weapons? Did they appreciate the dangers of provoking the country's ruler with social media posts and military exercises? Did the tragic milestones of that fateful month – North Korea's accidental shoot-down of Air Busan flight 411, the retaliatory strike by South Korea, and the tweet that triggered vastly more carnage – inevitably lead to war? Or did America's leaders have the opportunity to avert the greatest calamity in the history of our nation?

'Answering these questions will not bring back the lives lost in March 2020. It will not rebuild New York, Washington, or the other cities reduced to rubble. But at the very least, it might prevent a tragedy of this magnitude from occurring again. It is this hope, more than any other, that inspired The 2020 Commission Report.'

'You might think twice about keeping this novel on your bedside table, if you're prone to night sweats,' writes the reviewer from the *Globe & Mail*.

https://www.nonproliferation.org/the-2020-commission-report-on-the-north-korean-nuclear-attacks-against-the-united-states/

Look Down Under for uplift on financial crime

Writing for the Royal United Services Institute ('RUSI'), Tom Keatinge, director of the Institute's Centre for Financial Crime and Security Studies, argues that the UK 'should learn from Australia and become a global leader in the provision and coordination of technical assistance by turning its financial crime-fighting focus abroad.' Keatinge says that while some headway has been made in fighting financial crime in the past two years, 'For all the new acronyms, strategies and focus, thus far the bulk of the effort applied by the UK has been domestically focused, to ensure the UK is a "hostile environment" for criminal finances; and more specifically, the effort was undertaken to ensure the best possible review by the FATF whose report will be published in early December.'

Australia, he says, is showing the way ahead. 'Its FIU, AUSTRAC (Australian Transaction Reports and Analysis Centre), has an international strategy that includes capacity-building and partnership programmes for key regional FIU partners with AUSTRAC analysts embedded in, or forward-deployed to, a range of jurisdictions. In addition, Australia's Home Affairs department includes an Anti-Money Laundering Assistance Team that 'partners with countries in the Asia-Pacific region to strengthen laws and processes on anti-money laundering, counter financing of terrorism and proceeds of crime in line with international standards', leveraging Australia's significant contribution to the running of the FATF-style regional body in the Asia-Pacific region...

'The recipients across the Asia-Pacific region ... have viewed Australia's efforts favourably. This form of soft power has delivered results and strengthened relationships.

'These programmes require the long-term commitment of (limited) funding, resources and, above all, leadership.'

IRELAND

Bill prohibiting trade in settlement goods passes upper house of Irish parliament

By Cormac Little, William Fry

www.williamfry.com

In July 2018, the Control of Economic Activity (Occupied Territories) Bill 2018 (the 'Bill'), a private member's bill proposed by the Irish independent senator Frances Black, was passed in the Seanad (the upper house of the Irish parliament). The Bill makes it an offence for a person to import or sell goods or services originating in an occupied territory or to extract resources from an occupied territory in certain circumstances.

Although the Bill does not expressly refer to Israel or Palestine, it has been widely interpreted as being directed at restricting trade with Israeli settlements.

The Bill would apply to:

- a person who is an Irish citizen or ordinarily resident in the State,
- a company incorporated under the Companies Act 2014, and
- an unincorporated body whose centre of control is exercised in Ireland.

The vote was passed by 25 votes to 20 in the Seanad, despite opposition from the Irish government. The Bill will next pass through the Dáil (the lower house of the Irish parliament) to be debated and voted on. If passed in the Dáil, the Bill will become law, subject to being approved and signed by the President of Ireland.

SINGAPORE

What should businesses look out for when the US reintroduces sanctions on Iran?

By Chian Voen Wong (Mayer Brown Consulting (Singapore) Pte. Ltd.)

www.mayerbrown.com

On 16 January 2016, the Joint Comprehensive Program of Action (JCPOA)[1] was implemented in accordance with the Iran nuclear deal concluded on 14 July 2015 as a result of the negotiations between China, France, Germany, the Russian Federation, the United Kingdom, the United States, the EU and the Islamic Republic of Iran.

The landmark deal lifted international sanctions on Iran,[2] although restrictions remained on certain activities.

Consequently, the Monetary Authority of Singapore ('MAS') issued the MAS (Sanctions and Freezing of Assets of Persons – Iran) Regulations 2016, lifting Singapore's sanctions on Iran effective 17 June 2016, in accordance with UNSC resolution 2231 (2015). At the same time, the Regulation of Imports and Exports (Amendment) Regulations 2017 allowed Singapore businesses to resume trade with Iran.

The US withdraws from JPCOA

On 8 May 2018, the United States announced its decision to withdraw from the JPCOA and re-impose 'secondary' sanctions targeting non-US person[3] dealings relating to Iran sanctions in two tranches.

i. *Starting from 6 August 2018:* Re-imposition of all secondary sanctions lifted under the nuclear deal except those stated in (ii) below, including transactions relating to Iran's automotive sector, industrial and raw materials, trade in gold and precious metals, the Iranian government's purchase or acquisition of US dollar banknotes, the purchase or sale of Iranian rials and Iranian sovereign debt.

The US will also block the export and re-export of commercial passenger aircraft and related parts and services and the importation of certain Iranian products.

The US President issued Executive Order of 6 August 2018 'Reimposing Certain Sanctions With Respect to Iran' to implement the first tranche of re-imposed US sanctions against Iran, effective 7 August 2018.

ii. *Starting from 4 November 2018:* Re-imposition of secondary sanctions targeting certain energy,

financial, insurance and shipping-related activities.

In addition, the government of Iran and various persons and entities previously removed pursuant to the JCPOA will be re-added to the US Department of the Treasury, Office of Foreign Assets Control ('OFAC')'s List of Specially Designated Nationals ('SDN List').

The 8 May announcement and the two waiver periods described above do not impact other significant US sanctions and export control restrictions that have been in place throughout the nuclear deal, including the primary US trade embargo against Iran, US export controls and certain secondary sanctions that remained intact under the JCPOA.

Reactions of other countries

The US withdrawal came despite the concerns of many other countries, including the other parties to the JCPOA. To date, all other UN members continue to adhere to UNSC resolution 2231 (2015), including Singapore. In fact, the European Union announced the activation of its Blocking Statute,[4] intending to 'shield' EU nationals, EU residents, EU-incorporated companies, non-EU nationals or entities acting professionally in the European Union, and EU-controlled shipping companies domiciled outside the European Union from the extra-territorial reach of the US sanctions laws on Iran. The EU blocking statute also comes into force 7 August 2018.

What is Singapore's response?

Following the implementation of the JCPOA, Singapore lifted its Iran sanctions, in accordance to the UNSC resolution 2231 (2015):

i. *2016 MAS Regulations on Iran* – Financial institutions in Singapore are not prohibited from providing financial assistance such as investment, brokering, other financial services or other related services, including insurance or reinsurance, funds, financial assets, economic resources transfer services to:
   - o The Iranian government;
   - o Iranian nationals;
   - o Entities incorporated in Iran or subject to its jurisdiction;
   - o Individuals or entities acting on behalf of, or on the direction of, any of the three persons identified above; and
   - o Entities owned or controlled, directly or indirectly, by any of the three persons identified above.

Prohibitions remain on 'designated persons' identified in the UN List, as well as on 'sanctioned activities' related to the design or technology of ballistic missiles capable of delivering nuclear weapons. Prohibitions also remain on 'designated items' including any item which could contribute to uranium reprocessing or enrichment related or heavy water related activities.

Taking actions to mask an Iran-related transaction and inducing a US entity or person to be involved can expose the business to severe penalties for breaching US sanctions.

Non-financial institutions and natural persons in Singapore are similarly subject to the sanctions requirements.

ii. *Regulation of Imports and Exports (Amendment) Regulations 2017* – Singapore allows the trade in non-prohibited goods with Iran, subject to a customs permit requirement. Import of arms and related materials from Iran, and the export of 'designated items', which are items that could contribute to the development of nuclear weapon delivery system and arms and related materials to Iran, continue to be prohibited.

Following the US decision to withdraw from the JCPOA, Singapore has not reinstated the Iran sanctions. In general, Singapore does not enforce unilateral sanctions adopted by other countries, such as the US. Accordingly, the abovementioned provisions remain in force.

The reality for businesses in Singapore

With the lifting of the Iran sanctions, the Singapore government has been active in promoting bilateral ties with Iran, including signing a bilateral investment treaty ('BIT') and encouraging Singapore businesses to venture into Iran.

However, Singapore companies could be hit by the extra-territorial application of the US sanctions. We identify a few of the practical implications below.

i. The US market is one of Singapore's largest export markets. Only Singapore businesses which do not have links with the US market (whether through physical presence, financial ties or through supply and distribution chains) will be able keep their access to the Iranian market.
ii. The US dollar is the basis of a large proportion of trade in Singapore. Settlement of transactions involving Iran may not be denominated in US dollars. In addition to the existing restrictions on US dollar-denominated transactions involving Iran, the secondary sanctions are expected to target some of Iran's most significant financial institutions. This will significantly complicate payment arrangements that may expose Singapore companies to potential commercial risk in addition to the risk of secondary sanctions associated with such trade.
iii. The global importance of the US financial system and the international nature of Singapore's financial system mean that many banks do not want to deal with Iran even though the transactions are completely legal in Singapore. This makes it a great challenge for Singapore businesses to gain access

Links and notes

[1] On 20 July 2015, the Security Council unanimously adopted resolution 2231 (2015) endorsing the JCPOA. The JCPOA was implemented after the UN Security Council received the report from the International Atomic Energy Agency ('IAEA') confirming that Iran has complied with specific requirements.

[2] Sanctions imposed under UNSC resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010) were terminated.

[3] Non-US persons include non-US subsidiaries of US persons. US persons generally include US citizens and permanent residents; entities organised under US law, including foreign branches; and any person located in the United States.

[4] Council Regulation 2271/96, also referred to as the 'Blocking Statute', was initially adopted to 'oppose' the extraterritorial reach of the US' Helms-Burton Act and 1996 Iran-Libya Sanctions Act (ILSA).

to trade finance, credit facility, insurance, etc.

iv. Many carriers want to avoid being caught up in the US sanctions. Singapore businesses may have difficulties finding container lines that would ply the Iran-Singapore trade lane.

Businesses should take compliance with US sanctions and export control laws seriously. Taking actions to mask an Iran-related transaction and inducing a US entity or person to be involved can expose the business to severe penalties for breaching US sanctions. At the same time, not all transactions involving Iran will subject Singapore entities to sanctions exposure.

It is advisable that Singapore companies with interests in the Iranian market carefully assess the risks associated with their respective activities.

RUSSIA

Response to US sanctions – Russia may take moderate approach

By Hannes Lubitzsch and Tatiana Dovgan, Noerr

www.noerr.com

Russia's response to the latest US sanctions is still in the process of being formed. However, the Russian state now seems to be refraining from extreme measures such as the earlier proposed introduction of criminal liability for sanctions compliance.

A more moderate approach is suggested by the recent counter-measures:

1. considerations by the State Duma to introduce administrative liability for sanctions compliance instead of criminal liability;
2. the entering into force of a framework law for counter-measures against the United States and other 'unfriendly states';
3. the increase of import customs duties for certain goods originating from the United States to counter increased US tariffs; and
4. the extension of the 2014 import ban for agricultural products from the United States and the European Union.

Ongoing consideration of blocking legislation

The draft blocking law, which was adopted on its first reading by the State Duma on 15 May 2018, proposed criminal liability of up to four years' imprisonment for individuals who comply with foreign sanctions and thereby restrict the ordinary business operations of Russian persons. In addition, it proposed that deliberate actions by Russian citizens which facilitate the introduction of foreign sanctions shall be punishable by up to three years' imprisonment.

While criminal liability for the facilitation of the introduction of foreign sanctions will likely become law,[1] the initiative to introduce criminal liability for compliance with the sanctions seems to have lost support. In particular, the Russian President stated that Russia will not punish foreign partners for complying with anti-Russia sanctions – this question had been decided.[2] Also, the State Duma no longer seems to be pushing criminal liability and is now considering only the less severe form of administrative liability for sanctions compliance.[3] To date, however, no draft law for such an administrative liability has been presented. These developments indicate that any upcoming liability for sanctions compliance will likely be significantly less severe than initially proposed.

New framework law for counter-measures

The Federal Law No. 127-FZ 'On measures (counter-measures) in response to unfriendly actions of the United States [...]' entered into force on 4 June 2018. This law constitutes another basis for the Russian President to take extensive economic counter-measures against the United States and other 'unfriendly states' supporting the anti-Russia sanctions. In contrast to measures according to the Federal Law No. 281-FZ 'On special economic measures' of 30 December 2006 (please see below), counter-measures under this law can be unlimited in time. Import bans can be imposed for any goods originating from unfriendly states or produced by companies incorporated in these states, except for goods which are life-saving and have no equivalent produced in Russia.

The taking of any counter-measures is still at the sole discretion of the Russian President. However, counter-measures under this law have to date neither been taken nor proposed.

Increase of import duties on certain US goods

Governmental Order No. 788 of 6 July 2018 increased the import customs duties for certain types of goods originating from the United States to rates ranging from 25% to 40%. These types of goods include means of transport for the carriage of goods, road construction machinery, oil and gas equipment, metal processing and rock-drilling equipment as well as optical fibre. The new import customs duties will apply from 6 August 2018.

This measure is intended to counter the increase of US import tariffs on steel (to 25%) and aluminium (to 10%) originating from Russia and other states, which has been in effect since 23 March 2018. It is therefore not a counter-measure under the new framework law (please see above), but

a measure based on the principles of the World Trade Organisation ('WTO'), the Treaty on the Eurasian Customs Union and Federal Law No. 164-FZ 'On the fundamentals of state regulation of foreign trade activity'.

Extension of import ban for agricultural products

Based on Presidential Decree No. 420 of 12 July 2018 and Governmental Order No. 816 of the same date, the import ban on agricultural products, raw materials and food from the United States, Member States of the European Union and other states supporting the anti-Russia sanctions has been extended for the time period from 1 January to 31 December 2019.

This import ban was initially imposed on 7 August 2014 for one year and has since then been regularly extended. It is based on Federal Law No. 281-FZ 'On special economic measures' of 30 December 2006 which authorises the Russian President to take temporary measures to respond to unfriendly actions of foreign states which threaten the interests of the Russian Federation.

Links and notes

[1] See, for example: https://www.gazeta.ru/politics/2018/06/19_a_11807005.shtml?updated

[2] See, for example: https://www.rbc.ru/business/26/05/2018/5b0872619a7947339498aedc?story=5af980859a7947b069a0a9d3

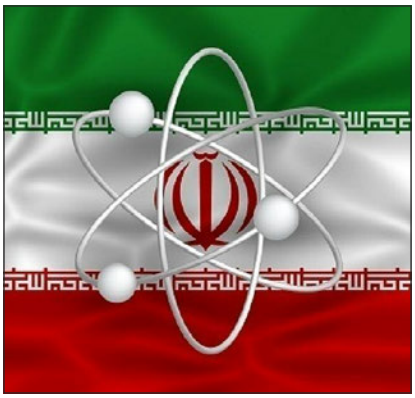
[3] See, for example: https://www.vedomosti.ru/politics/news/2018/07/10/775124-volodin-sanktsii

IRAN

EU blocking statutes, Iran sanctions, and the businesses caught in between

By Reid Whitten, Sheppard Mullin Richter & Hampton

www.sheppardmullin.com



Imagine telling your company's board of directors that the company will have to knowingly violate the law. Further, you might note, the American Law Institute's Principles of Corporate Governance state that, with very limited exceptions, a director who knowingly causes the corporation to disobey the law violates his duty of care. The protections of the Business Judgement Rule may not be available to a board member who, charged with navigating the Scylla and Charybdis of a conflict of laws, steers right into the shoals of noncompliance.

Beginning 6 August, that will be the situation facing the thousands of companies that are subject to US sanctions on Iran and to EU regulations blocking those sanctions. While it appears to be a stark choice, some nuances to the regulations may make navigating the narrow straights of the conflict of laws a less Odyssean and more practically manageable task.

The rock: US secondary sanctions with extraterritorial applications

Beginning 6 August, the United States will begin enforcing certain secondary sanctions applicable to Iran pursuant to the US withdrawal from the Iran nuclear agreement known as the Joint Comprehensive Plan of Action ('JCPOA'). The United States will reimplement the rest of the secondary sanctions after 4 November 2018.

Secondary sanctions are those that apply to transactions with no US nexus: where a non-US company deals with Iran outside of the United States and not involving US persons or the US banking system. Non-US companies that violate secondary sanctions are subject to being sanctioned themselves by the US government. Non-US financial institutions that violate secondary sanctions are subject to restrictions or prohibitions on US correspondent or payable through accounts (read: restricting their access to the US dollar).

The hard place: EU Blocking Regulation

On 6 June 2018 the European Commission adopted an amendment to its Blocking Regulation (originally propounded to block the effect of US secondary sanctions on Cuba) to counteract the effects of the extraterritorial application of US sanctions on Iran. Broadly, the resolution's main provisions are as follows:

- *Coverage:* Natural and legal persons resident or organised in the EU that engage in international trade or commercial activities.
- *Requirements*: Covered persons affected by US sanctions on Iran must report to the European Commission.
- *Prohibitions:* Covered persons are prohibited from complying, directly or through a subsidiary or intermediary, actively or by deliberate omission.
- *Rights of action:* EU persons have the right to recover any damages, including legal costs, where those damages arise from a covered person's compliance with US sanctions on Iran. Recovery could take the form of 'seizure and sale of assets held by those persons or entities.' (EC No 2271/96, Art. 6)
- *Penalties:* Each EU Member State is tasked with deciding the penalties for breach of the Blocking Regulation. The regulation merely requires that sanctions be 'effective, proportional and dissuasive'.

Shooting the gap: EU authorisation to comply with US law

Article 5 of the EU blocking resolution states that covered persons may be authorised by the Commission to comply with US sanctions on Iran

where there is sufficient evidence that non-compliance would cause serious damage to a natural or legal person. The resolution does not state how companies go about applying for that authorisation. However, our (rather persistent) calls to our contacts in the Commission offices (finally) yielded the following response:

The criteria for the application of the second paragraph of Article 5 will be laid down in a Commission Implementing Regulation that will also be published and will enter into force on 7 August.

It is not clear how long the application approval process may take or the likelihood of approval, but an authorisation form and guidance were published on 7 August.

The process does provide companies at least a theoretical easing of their conflict of laws dilemma. Although the authorisation application does not have a suspensive effect on the Blocking Regulation, if a company applies for authorisation to comply with US regulations, then continues to comply with US regulations, it is possible that the company's good faith efforts to comply with both applicable legal regimes may mitigate its risks with respect to potential prosecutions by the government or suits for damages from affected persons.

However, application brings with it the same risk that a company notifying the Commission of its US sanctions issues: it alerts authorities that the company may be in violation of the Blocking Regulation. Further, where the Commission rejects a company's application for authorisation to comply with US sanctions, that company may feel doubly threatened, as the Commission and, presumably, domestic regulators will be aware that the company has continued to comply with US sanctions.

The lesser of two evils: risk mitigation where risk elimination is impossible

According to Homer, Odysseus steered close to the monster Scylla, losing only a few sailors, rather than the whirlpool Charybdis, where he risked the loss of his entire ship. Companies may face a similar choice of which regulator is scarier, and that choice is clear. The penalties for violating the EU Blocking Regulation depend on the domestic application in each EU Member State, but for many multinational companies, none of those potential penalties comes close to the devastation possible pursuant to US secondary sanctions enforcement. The effect on a multinational business of being prohibited from any transaction with US persons – no importing, no exporting, and, generally, no use of US dollars – could be a death sentence. It could be equally injurious to a foreign financial institution with international customers to be cut off from access to the US banking system.

For that reason, many companies will be tempted to honour the EU Blocking Regulation in the breach. However, on a case-by-case basis, companies may identify ways to manage the risks of doing business under both legal regimes based on the particular facts of their business arrangements.

We recommend that subject companies discuss the conundrum with experts in US and EU law (and the law of their particular EU member state) to develop a plan to navigate the narrow passage between US sanctions and the EU Blocking Regulation. The one solution that neither we, nor Homer, would recommend, is sailing straight ahead without a plan, blind to the dangers and exposed to the risks.

USA

Enhanced controls for emerging and foundational technologies

Daniel J. Gerkin and David R. Johnson, Vinson & Elkins

www.velaw.com

The President has signed the National Defense Authorization Act of 2019 ('NDAA'), which, in addition to expanding the jurisdiction of the Committee on Foreign Investment in the United States ('CFIUS') to review foreign direct investment, implements the Export Control Reform Act of 2018 ('ECA'), which sharpens the focus of the US government on emerging and foundational technologies that are deemed not to have been adequately addressed by the prevailing US export control regimes. The NDAA also places limits on the procurement of equipment and services from certain Chinese entities, though certain members of Congress had adamantly advocated for much more stringent restrictions.

Export Controls Act of 2018

Permanent statutory authority for US export controls

With limited exceptions, the ECA repeals the Export Administration Act of 1979, which lapsed several years ago and has been statutorily authorised each year since pursuant to executive orders issued under the International Emergency Economic Powers Act ('IEEPA'). Accordingly, the ECA now serves as the permanent statutory authority for the US Export Administration Regulations ('EAR'), which generally govern the export, reexport, and in-country transfer of commercial and dual-use commodities, software and technology, and which are administered by the Bureau of

Industry and Security, US Department of Commerce ('BIS').[1]

Treatment of emerging and other types of critical technologies

In addition to ensuring permanent statutory authority for the existing commercial and dual-use export controls regime, the ECA directs the President, in coordination with the departments of Commerce, Defense, State, and Energy to develop a 'regular and robust process to identify the emerging and other types of critical technologies of concern and regulate their release to foreign persons as warranted regardless of the nature of the underlying transaction.' Specifically, these agencies are tasked by the ECA with identifying 'emerging and foundational technologies' that are essential to the national security of the United States, but which are not currently controlled for export purposes.[2]

The process for identifying such technologies will be informed by publicly available information, classified information, information arising out of the CFIUS review process, and information generated by the various BIS advisory committees, and will take into account the development of such technologies in foreign countries, the effect export controls might have on continuing US development efforts, and the effectiveness of export controls with respect to limiting the proliferation of such technologies to foreign countries.

The identified technologies will, following a notice and comment period, be subjected to enhanced US export controls, possibly to include licensing requirements, and will be proposed for inclusion in multilateral export control regimes. At a minimum, licences will be required for countries subject to a US embargo, including those that solely are arms embargoed, such as China.[3] Please note that licence applications submitted by or on behalf of a joint venture, joint development agreement, or similar collaborative arrangement may require the identification of any foreign person with a significant ownership interest in a foreign person participating in the arrangement.

The following activities will be excepted from any licensing requirements:

- The sale or lease of a finished item and the provision of associated technology if such items and technology are generally made available to customers, distributors, or resellers;
- The sale or licence to a customer of a product and the provision of integration or similar services if such services generally are made available to customers;
- The transfer of equipment and provision of associated technology to operate the equipment if the foreign person could not use the equipment to produce critical technologies;
- The procurement by a US person of goods or services, including manufacturing services, from a foreign person if the foreign person has no rights to exploit any technology contributed by the US person other than to supply the procured goods or services; and
- Contributions and associated support provided by a US person to an industry organisation related to a standard or specification, whether in development or declared, including any licence of, or commitment to license, intellectual property in compliance with the

rules of any standards organisation.

The ECA requires reporting to Congress and to CFIUS every 180 days regarding actions taken to identify and control emerging and foundational technologies.

Changes to licensing process

The ECA mandates that applications for licences address 'the impact of a proposed export of an item on the United States defense industrial base' and an assessment of whether 'the denial of an application for a license or a request for an authorization of any export that would have a significant negative impact on such defense industrial base.' By significant negative impact, the ECA means:

- 'A reduction in the availability of an item produced in the United States that is likely to be acquired by the Department of Defense . . . for the advancement of the national security of the United States, or for the production of an item in the United States for the Department of Defense . . . for the advancement of the national security of the United States.'
- 'A reduction in the production in the United States of an item that is the result of research and development carried out, or funded by, the Department of Defense . . . to advance the national security of the United States, or a federally funded research and development center.'
- 'A reduction in the employment of United States persons whose knowledge and skills are necessary for the continued production in the United States of an item that is likely to be acquired by the Department of Defense . . . for the advancement of the national security of the United States.'

Like the IEEPA, the ECA authorises criminal penalties of up to $1 million and imprisonment for not more than 20 years.

Criminal and civil penalties

Like the IEEPA, the ECA authorises criminal penalties of up to $1 million and imprisonment for not more than 20 years. However, the ECA increases the current inflation-adjusted maximum civil penalty to the greater of $300,000 or twice the value of the underlying transaction. These also are the criminal and civil penalties set forth in the Anti-Boycott Act of 2018.

Treatment of certain Chinese telecommunications equipment manufacturers and service providers

Over the objections of Sen. Marco Rubio, among others, the NDAA ultimately did not reimpose sanctions on Chinese telecommunications equipment manufacturer and service provider, Zhongxing Telecommunications Equipment Corporation ('ZTE Corporation'), and certain of its affiliates, which were subject to a BIS denial order arising out of US export control violations stemming from transactions involving Iran and North Korea. That denial order was terminated, effective 13 July 2018. The ECA does, however, prohibit federal agencies from procuring or obtaining, or entering into contracts with entities using, equipment, systems, or services that, in turn, use Chinese-origin telecommunications equipment or services deemed to be a 'substantial or essential component of any system' or 'critical technology as part of any system.'

The targeted Chinese-origin telecommunications equipment or services are:

- Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities;
- For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Technology Company, Dahua Technology Company, or any subsidiary or affiliate of such entities;
- Telecommunications or video surveillance services provided by any of the above-named entities or using the above-described equipment; and
- Telecommunications or video surveillance equipment or services produced or provided by an entity reasonably believed to be owned or controlled by, or otherwise connected to, the Chinese government.

Links and notes

[1] The EAR also encompass the regulations that govern the participation of U.S. persons in unsanctioned foreign boycotts. These regulations now are permanently authorized by the Anti-Boycott Act of 2018.

[2] Please note that the EAR currently allow for the imposition of temporary controls on items in accordance with their interim classification within Export Control Classification Number 0Y521.

[3] The ECA also requires a review of the current controls on exports, reexports, and in-country transfers for military end uses and military end users in U.S. and United Nations arms-embargoed countries, as well as a review of the Commerce Control List of items that currently are not subject to any licensing for U.S. arms-embargoed countries.

FRANCE

French customs announces customs/licence application 'link'

By Raphael Barazza

rb@customs-lawyer.fr

French customs has, in Customs Official Bulletin N°7245 of 29 June 2018, announced a new online link ('GUN') between the online licensing service ('EGIDE') and the online customs declaration service ('Delt@-G').

The Directorate-General of Customs and Excise ('DGDDI') and the Department of Dual Use Goods now share a common platform, via the National Single Window for Customs Clearance ('GUN'), between the DELT@-G customs clearance system and the EGIDE application where the export licences of dual-use goods are stored in electronic format.

This link has been effective as of 18 June 2018. Exporters, customs and licensing officers should all benefit from the development, which has three objectives:

1. For economic operators, paperless (electronic) DUI export licences speed the process of customs clearance, notably by reducing delays in the detention of goods at customs. In addition, the EGIDE portal offers a platform for tracking values and quantities for individual licences.
2. For customs services, the link enables the automation of documentary checks between the customs declaration and the SBDU licence. This change reinforces the security of customs controls necessary for such sensitive goods.
3. For the SBDU, the implementation of the GUN establishes a better export tracking system of the licences it issues.

It should be noted that not all licences are eligible for the GUN interconnection between DELT@-G and EGIDE. The eligibility conditions differ according to the type and issue date of the licence.

Exporters of dual-use items no longer have to submit the hard copy of the export licence for products to customs when it concerns:

- French general licences and European general authorisations.
- Individual and global licences, issued by the SBDU as of 18 June 2018 to operators registered on EGIDE.

Individual licences are automatically transferred to EGIDE as soon as Delt@-G issues a voucher ('BAE)'.

However, the procedure for using a paper-based licence at the customs office for visas and charging for individual licences/export tracking for global licences remains in place for:

- Individual and global licences issued by the SBDU, before 18 June 2018, to operators registered on EGIDE;
- Individual and global licences issued by the SBDU, before or after 18 June 2018, to non-registered operators on EGIDE;
- Individual licences for temporary exports (via Delt@-G or ATA carnet) regardless of the issue date and whether or not the operator is registered on EGIDE.

In addition, the move to electronic licences does not affect existing legislation, indeed the processing of licences and authorisation applications are still regulated by Council Regulation 428/2009, while all procedures and forms remain unchanged.

We need to talk about Saudi

In early September, the Saudi-led coalition that bombed a bus, killing 40 Yemeni children on the way to a picnic, admitted that the strike was 'unacceptable,' (reversing an earlier statement that the action was 'legitimate' and carried out in accordance with humanitarian law).

The incident didn't receive the coverage that it arguably should have, unfortunately, partly because Yemen is now so dangerous, its infrastructure so destroyed and dilapidated that the numbers of press present to report back are very small – and they can't be everywhere all of the time.

Another reason is because this is a war that is tacitly supported by Saudi's sponsors, including the United Kingdom and United States, neither of which have any interest in alerting the world to its injustices or complexities – especially against a backdrop of lucrative arms sales.

But, is it good for business if companies find that the weapons they manufacture have killed innocents? And what is the purpose of export controls if they do not prevent just that? Whether our governments want to or not, it is likely that they will have to reappraise their role in the Saudi-led campaign in Yemen (or failing that, justify it in clear terms). The people that I speak to in the compliance function are keenly aware of the ethical dimension of export controls, and how that doesn't always align neatly with government policy.

Is it good for business if companies find that the weapons they manufacture have killed innocents?

September means back to school, and back to the Brexit headache. We learn, helpfully, from the UK government that 'in the event of a no-deal', the European Court of Justice would issue an open licence for exports from the UK to the EU, but that EU-issued licences would no longer be valued for exports from the UK. *WorldECR* has asked the UK's Department of Trade how many exporters it believes would be affected by the change (and how a 'no-deal' Brexit would differ in this regard from a 'some-kind-of-a-deal' Brexit), but is only so hopeful of receiving an answer...

Training day

We're delighted to be working with award-winning export controls consultants, Strong & Herd, on a two-day export controls training programme to be held in London in November (see the full-page notice in this issue). The comprehensive programme will cover everything from the basics – the UK export control system; the difference between dual-use and military; record keeping and so on – through licensing, end-user controls, catch-alls, sanctions, to discussing where best to site the function for it to be most effective. The training should appeal to those who are new to export controls and also to those who have a few licences under their belts! We look forward to seeing you there.

Tom Blass, September 2018
TNB@worldecr.com

Establishing an effective export compliance organisation

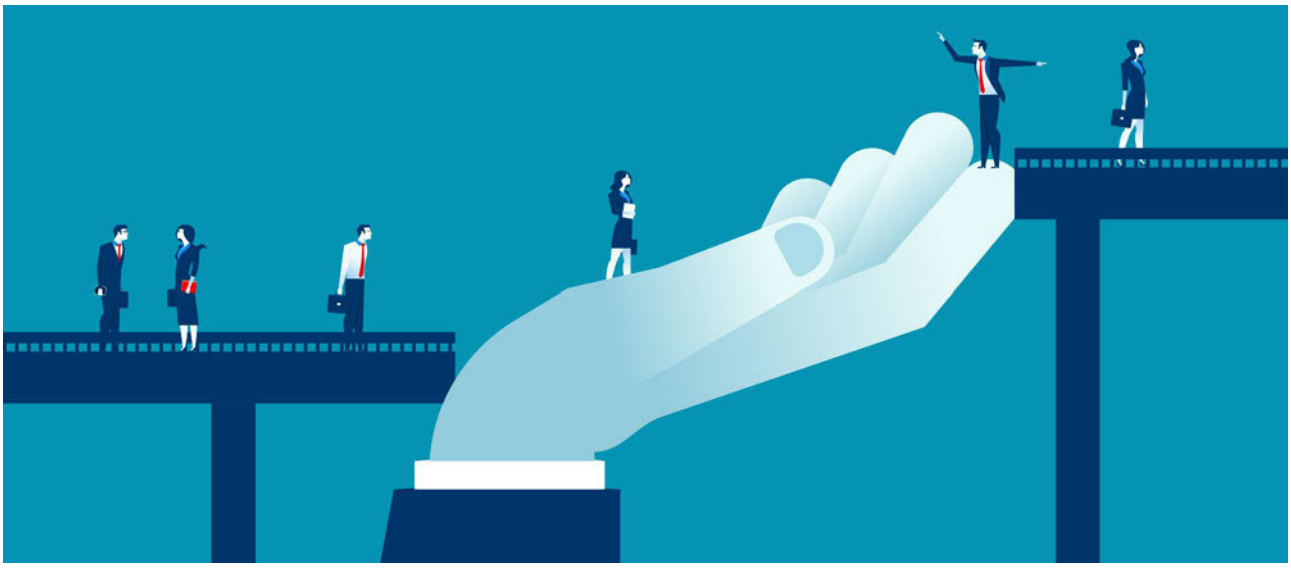
Where should the export control compliance team sit within the organisation to make it most effective? There is no one-size-fits-all solution, writes Julia Bell. Rather, the decision will rest on the individual needs of the particular organisation.

Many companies are seeking to understand the structural strengths and weaknesses of different export compliance organisational models with respect to scope and mandate of the export control function, allocation of accountability across divisions and geographies, and relationship with the business served. When it comes to determining where export compliance should sit within an organisation, there is no 'one-size-fits-all' approach. Export compliance organisation reporting lines vary depending on the size and complexity of the organisation, its global footprint, the sensitivity of its products and its routes to market. The most natural home for the export controls function is to sit in Compliance and report to the Board via Compliance/Legal, which is typical in highly regulated industries such as Aerospace and Defence. In doing so, the General Counsel of the company gains better visibility and line of sight of export compliance risk exposure. In this structure, it is critical to ensure that the export compliance procedures set by Legal are effectively translated into business requirements that can be understood and embedded at an operational level. In other words, there should be a plain English articulation of requirements, avoiding 'legalese' at all costs.

Export compliance is widely perceived to add more value to the business when the export compliance function is treated as a strategic partner.

At other organisations, export compliance will report into Supply Chain – however we frequently see issues with this approach. In this structure, the risk is that export compliance activity will focus on physical movement of goods, and intangible exports, such as technology/software transfers will be subject to less rigorous oversight. There is also potential for conflicts of interest that might inhibit fulfilment of the compliance agenda, where employees will choose to act in the commercial interests of the business rather than taking tough decisions to ensure compliance. In our experience, the authority for decision-making and oversight must be separate to the commercial operations of the business. Therefore, if there is no Legal or Compliance function (for example in a smaller organisation), we would recommend export compliance sits in Finance, where there is typical accountability for the company's internal controls.

Regardless of its organisational reporting lines, export compliance is widely perceived to add more value to the business when the export compliance function is treated as a strategic partner. All core processes in the value chain can be impacted by export controls, and if the export compliance function is not adequately structured and resourced to embed export compliance into day-to-day activities, it loses credibility within the organisation. Consequently, there is a cross-industry drive to increase the visibility of the export compliance



function and attract top talent to create a partnership with the business and contribute new value to the organisation. This can be accomplished in the following ways:

Re-structuring the export compliance function

Many organisations are restructuring the export compliance function to provide more credibility and influence by reporting to the General Counsel, Chief Compliance Officer, or directly to the CEO. With leadership alignment on key principles, the export compliance team can then establish effective mechanisms for communication, escalation and decision-making, and focus on embedding export compliance requirements into day-to-day business activities.

Developing and enhancing career paths for trade compliance professionals

Companies are focusing on creating a platform to attract and retain top talent within a legal and compliance environment by consolidating positions in a centralised function to allow for more specialisation and clearer progression. Competencies are published by grade, key performance indicators allow for better evaluation of the progression of compliance personnel, and compliance is equalised against sales targets through updated performance management and reward strategies. Where there is a challenge to recruit experienced talent, companies can consider introducing rotation programmes, rotating staff between commercial, internal audit and export compliance functions to develop expertise and provide career opportunities.

There is no single right 'home' for the export compliance function within an organisation.

Alignment with other legal and compliance areas to leverage skillsets, information and avoid duplication

Legal and regulatory obligations can be seen as disruptive, rather than enabling, to the business, because requirements are continuously layered on to the business from multiple areas. By coordinating with other legal and compliance areas such as anti-bribery and corruption, ethics, anti-trust, and anti-money laundering/financial crime, you can simplify the handover to the business and avoid duplication of requirements, creating a 'lean' approach to compliance.

There is no single right 'home' for the export compliance function within an organisation. What is critical is that the function is structured and governed effectively, and is able to attract and retain talent that have sufficient seniority, influence and resource to drive the compliance agenda.

Julia Bell is a senior manager in Deloitte's Global Export Controls & Sanctions team in London.

julbell@deloitte.co.uk

Turkish delight: sanctions, tariffs, and the new normal

Increasingly, tariffs and sanctions are the tools of contemporary statecraft – and we'd best get used to that, writes Dr Scott A. Jones.

'All that is solid melts in air...,' and so go the political-economic certitudes of the post-World War Two global order. The international house the US built is being sundered by her own hand. In addition, others are adopting the emerging global *modus operandi* – economic statecraft – perhaps hastening what economist Paul Krugman referred to as the 'great unraveling'. While a death foretold may be premature, we can assuredly see that sanctions are flying. States are increasingly reaching for economic levers to achieve foreign policy objectives, which is a working definition of economic statecraft.

In a March 2018 *Times of Japan* editorial, Japanese scholar Toshifumi Kokubun noted: 'Beijing's suspension of rare earths exports to Japan in the wake of the 2012 dispute over the Senkaku Islands or its cutoff of tourist groups to South Korea following Seoul's decision to deploy a missile defense system in contravention of Chinese wishes are two examples of the use of economic statecraft for political purposes. Japan must become sensitized to and creative in the use of such statecraft.'

The latest instance of unravelling and economic statecraft is the curious case of Turkey and its otherwise stalwart treaty ally, the United States. On 20 August, the Trump administration imposed sanctions on two Turkish government officials over the detention of an American pastor being held on espionage charges, the immediate effect of which was to further deflate the already enfeebled Lira. President Recep Tayyip Erdogan's characterisation of the sanctions is illustrative of the abovementioned trend, describing, in a recent speech, the strong United States dollar as among 'the bullets, cannonballs and missiles' foreigners are using to wage 'economic war' on Turkey.

In an opinion piece published in *The New York Times* on 10 August, President Erdogan continued the jeremiad about the ruinous use of economic levers to punish a 'shoulder to shoulder' ally. Trump tweeted his threat to raise tariffs on Turkish aluminium to 20% and steel to 50% just a few hours after the publication of Erdogan's op-ed, noting that the Turkish currency 'slides very rapidly downward against our very strong Dollar!' The United States is the biggest destination for Turkish steel exports, with 11% of the Turkish export volume. The Lira fell further after Trump's tweet. In response to US threats, Erdogan's government announced that it would be implementing retaliatory tariffs on American cars, alcohol, tobacco, and over 100 other products. Not to be left out of the fun, on 23 August, Congress blocked the proposed sale of 100 F-35s until the Pentagon issues a report assessing the 'overall strategic relationship with Turkey'.

States are increasingly reaching for economic levers to achieve foreign policy objectives, which is a working definition of economic statecraft.

Like much about the current administration, the petulant and profligate use of sanctions and tariffs is unprecedented. The Turkish case is particularly unique insofar as the administration is not only gut-punching a NATO ally, but doing so to curb Ankara's perceived wayward behaviour through economic statecraft rather than the traditional diplomatic means. The list of aggrieving behaviour includes Turkish support of jihadist groups in Syria, cultivating closer relations with Iran, and contracting to purchase S-400 surface-to-air missiles from Russia, the use of which would compromise the strategic integrity of the aforementioned F-35s. Foreign economic policy is also most likely being used for domestic political purposes: as red meat to the evangelical vote, the administration is turning the economic screws on Ankara to free the American cleric in the lead-up to the November mid-term elections.

On 15 August, President Trump tweeted the following: 'Our Country was built on Tariffs, and Tariffs are now leading us to great new Trade Deals – as opposed to the horrible and unfair Trade Deals that I inherited as your President. Other Countries should not be allowed to come in and steal the wealth of our great U.S.A. No longer!'

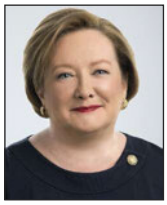
While not exactly correct in the broader US economy sense, the President is correct with respect to government revenue, at least until 1913 with the institution of income tax. Since the end of WW2, the US has promulgated and sponsored at considerable effort a free trade agenda with sanctions serving as a non-military, discrete adjunct to foreign policy. Now, tariffs and sanctions are indiscriminately, inconsistently applied to a range of political and economic issues. The forsaking of its custodial responsibilities over the system it helped construct sets a larger tone and creates a leadership vacuum. If the emerging tools of contemporary statecraft are tariffs and sanctions, expect more and novel engagements between allies, frenemies and adversaries. As professor Kokubun notes above, 'Japan (or insert country of your choice) must become sensitized to and creative in the use of such statecraft.'

Dr. Scott Jones is a Non-Resident Fellow at the Stimson Center in Washington, DC and a principal at TradeSecure, LLC.

http://tradesecure.net/

US sanctions on Russia

US Congress threatens more sanctions against the Russian government



The proposed Defending American Security from Kremlin Aggression Act of 2018 ('DASKAA') seeks to expand Russia-related elements in last year's Countering America's Adversaries Through Sanctions Act ('CAATSA'). Barbara Linney reviews the proposed legislation and considers its potential impacts.

On the eve of the one-year anniversary of the Countering America's Adversaries Through Sanctions Act ('CAATSA'), the US Congress again threatened additional sanctions against the government of the Russian Federation, with the introduction in the Senate of a new bill that would, among other things, impose additional sanctions with respect to the Russian Federation. Title VI of The Defending American Security from Kremlin Aggression Act of 2018 ('DASKAA')[1] would expand CAATSA sanctions and require reports to Congress on the status of various aspects of CAATSA implementation and other Russia-related matters. Title III would require reports to Congress on the use of chemical weapons by the Russian Federation.

Familiar focus

The list of activities targeted for sanctions is a familiar one, and includes illicit and corrupt activities, support for energy projects and development of crude oil resources, financial and banking activities, cyber transactions, and use of chemical weapons.

If enacted, DASKAA would allow the administration 180 days to impose blocking sanctions on Russian parastatal entities, political figures, oligarchs and other persons that facilitate illicit and corrupt activities on behalf of President Putin, directly or indirectly, as well as persons acting for them or on their behalf. The sanctions would also extend to family members of such persons who derive significant benefits from the sanctioned activities and any persons, including financial institutions, who engage in significant transactions with the sanctioned individuals and entities.

The sanctions would extend to … financial institutions who engage in significant transactions with the sanctioned individuals and entities.

The proposed legislation would also target transactions related to energy projects and development of crude oil resources, with either delayed or immediate effect, depending upon the location of the targeted activities.

CAATSA menu-based sanctions[2] against persons who knowingly invest in an energy project outside of the Russian Federation would take effect 180 days after enactment of DASKAA. The affected projects would be those that are supported by a Russian parastatal entity or an entity owned or controlled by the Russian government if the total value of the project exceeds or is expected to exceed US $250 million.

CAATSA menu-based sanctions against any person who knowingly sells, leases or provides goods, services, technology, financing or support related to development or production of crude oil resources in the Russian Federation would take effect immediately upon enactment of DASKAA. Notwithstanding the immediate effect of the new sanctions, the departments of State, Treasury and Energy would have 90 days to publish a list of specific goods, technology, financing and support affected. Until then, only the broad parameters provided in the legislation would serve

US sanctions on Russia

as guidance – namely, a fair market value threshold of US $1 million (or an aggregate fair market value of $5 million during any 12-month period) below which sanctions would not be triggered; and a 'direct and significant' contribution to the development or production of crude oil resources in the Russian Federation, including any direct and significant assistance with respect to the construction, modernisation, or repair of infrastructure that would facilitate the development of such crude oil resources. Ongoing projects would be excluded from the requirement to impose sanctions, but, again, guidance on how the exception would be applied need not be issued until 90 days after the effective date of the new sanctions.

Focus on finance

Other provisions of DASKAA target Russian financial institutions and sovereign debt.

Upon enactment of DASKAA, the US government would have 90 days to block the property and interests in property of eight specified Russian financial institutions. This will mean that US persons (including banks) will be required to freeze any assets of the blocked financial institutions held by them, and refrain from entering into any transactions with them. This provision represents a marked departure from standard blocking procedures, which generally impose blocking with immediate effect and do not provide any 'early warning' to either the blocked party or US persons with whom the blocked party may be dealing in order to avoid asset flight.

Also within 90 days of enactment of DASKAA, regulations would be required to be issued prohibiting US persons from dealing in Russian sovereign debt issued on or after the date that is 180 days after enactment of DASKAA. As defined by the proposed legislation, Russian sovereign debt would include bonds with a maturity of more than 14 days, foreign exchange swap agreements with a duration of more than 14 days, and any other financial instrument with a duration or maturity of more than 14 days that is determined to be sovereign debt of the government of the Russian Federation or is issued by one of the Russian financial institutions targeted for blocking.

DASKAA also requires CAATSA menu-based sanctions against persons who engage in significant transactions with any person in the Russian Federation that has the capacity or ability to support or facilitate malicious cyber activities or is owned or controlled by, or acts for or on behalf of, such persons, directly or indirectly. These sanctions would take effect not later than 60 days after DASKAA becomes law.

The new legislation would also require reports on the status of determinations under various sections of CAATSA.

Putin and CAATSA

Subtitle C of Title VI of DASKAA requires various reports to Congress, including an updated report on oligarchs and parastatal entities; a report on the estimated net worth and sources of income of President Putin and his family members; a report identifying the most significant senior foreign political figures and oligarchs in the Russian Federation as determined by their closeness to President Putin; and a report on whether the Russian Federation meets the criteria for designation as a state sponsor of terrorism.

The new legislation would also require reports on the status of determinations under various sections of CAATSA, including with respect to significant activities undermining cybersecurity (CAATSA section 224); significant investments in Russian crude oil projects and foreign financial institutions who have engaged in significant transactions involving such investments (CAATSA sections 225 and 226); violations of sanctions targeting Russia or facilitation of significant transactions on behalf of persons subject to such sanctions (CAATSA section 228); unjust privatisation of state-owned assets (CAATSA section 233); and chemical weapon and other activities in support of Syria (CAATSA section 234). These requirements of the draft legislation clearly signal congressional frustration with the pace of CAATSA implementation.

Chemical weapons

Title III of DASKAA includes various findings with respect to use of chemical weapons and agents by the government of the Russian Federation and a statement of US policy, including with respect to its intention to deter the government of the Russian Federation from chemical weapons production through sanctions and other means. Within 30 days after enactment, the US Department of State would be required to submit a report to certain Congressional Committees regarding use of chemical weapons by the government of the Russian Federation and imposition of sanctions under US statutory authorities (the 'CBW sanctions'). However, these provisions of the draft legislation may have been rendered moot, at least in part, by the subsequent determination by the US Department of State that the government of the Russian Federation has used chemical weapons in violation of international law or lethal chemical weapons against its own nationals and related imposition of sanctions.[3] Having said that, some members of Congress may take issue with the extent to which the Department of State exercised its authority to waive certain of these mandatory sanctions, in whole or in part.

Magnitsky and cyber

DASKAA would also add the Sergei Magnitsky sanctions to the list of Russia-related sanctions that cannot be terminated without congressional review, and Title VII would require various other non-sanctions measures targeting Russia, including the extension of limits on importation of uranium from the Russian federation.

Finally, while not mentioning Russia specifically, Title IV of DASKAA would bolster cybercrime prevention, and Title V would enhance prohibitions against election interference. Related bills on these subjects have also been introduced separately.[4]

Further developments

DASKAA has been referred to the Senate Committee on Foreign Relations, but no hearings have yet been scheduled. Also moving slowly is the proposed Defending Elections from Threats by Establishing Redlines Act of 2018 ('DETER Act'),[5] another piece of

US sanctions on Russia

Links and notes

[1] S. 3336, A Bill to strengthen the North Atlantic Treaty Organization, to combat international cybercrime, and to impose additional sanctions with respect to the Russian Federation, and for other purposes, introduced in the Senate of the United States on 1 August 2018.

[2] See 'Significant US sanctions developments under the Trump administration', B. Linney and C Griffin, *WorldECR* issue 64, November 2017.

[3] See 83 Fed. Reg. 43723 (27 August 2018).

[4] See S. 3288 and S. 3311, introduced in the Senate on 26 July 2018 and 31 July 2018, respectively.

[5] S. 2313, a Bill to deter foreign interference in United States elections, and for other purposes, introduced in the Senate of the United States on 16 January 2018. See, also, H.R. 4884, a Bill to deter foreign interference in United States Elections, and for other purposes, introduced in the House of Representatives on 16 January 2018. H.R. 4884 has been referred to several committees but has not yet been the subject of hearings.

pending legislation that features more sanctions against the Russian Federation. The DETER Act was introduced in the Senate on 16 January 2018 but was not the subject of hearings before the Committee on Banking, Housing and Urban Affairs, to which it was referred, until 21 August 2018. Like CAATSA, these congressional initiatives are unpopular with the Trump administration, and it remains to be seen whether Congress will be placated by increased implementation of existing sanctions legislation, such as the recent CBW sanctions, or persuaded by ongoing discussions to revise pending legislation in a manner acceptable to the administration. In any case, with the US congressional mid-term elections on the horizon, it is unlikely that new sanctions legislation will be enacted this year, although the past few years have shown that such predictions cannot be made with any degree of confidence.

However, the damage to US and global businesses may be done. The climate of uncertainty resulting from relentless congressional pressure and a significant uptick in US deployment of secondary sanctions against Russia and Iran over the past year has caused both the global business community and US allies to implement risk mitigation strategies.

Although DASKAA pays lip service to the importance of coordinating sanctions against the Russian Federation with the European Union, the steady increase in sanctions threats and implementation over the past year appears to have provoked the opposite result, as talks designed to avoid collateral damage to European businesses are reported to be underway amongst European governments. If these efforts are successful, the United States may face considerable challenges to its successful use of sanctions as an instrument of foreign policy, while US businesses will continue to pay the costs of an uneven playing field that are the inevitable result of unilateral sanctions policy.

Barbara Linney is a Member in the International Department, of Washington, DC-based law firm, Miller & Chevalier Chartered.

blinney@milchev.com

US ramps up sanctions activities against North Korea in 2018


The past 12 months have seen OFAC step up its commitment to the enforcement of sanctions against North Korea, and all the signs suggest that this is a trend that will only continue, write Timothy O'Toole and Claire Rickard Palmer.

For many years, North Korea (officially known as the Democratic People's Republic of Korea or DPRK) has been the target of wide-ranging US and international sanctions aimed at deterring what regulators viewed as a variety of types of 'malign' conduct. In the autumn of 2017, US and international sanctions increased as the DPRK regime continued to test nuclear weapons in the Korean peninsula. The US issued Executive Order ('EO') 13810.[1]

The world placed a virtual embargo on North Korea, particularly with regards to oil and financing. Nonetheless, through much of this time period, enforcement actions were rare. For a variety of different reasons, many having to do with North Korea's relatively small size and limited involvement in the Western economy and financial system, US regulators did not appear to view North Korea as an enforcement priority.

That appears to have changed in the past year. The first sign of the change occurred in November 2017, when the US Department of the Treasury's Financial Crimes Enforcement Network (FinCen) designated China's Bank of Dandong as a 'primary money laundering concern,' based on FinCen's determination that the bank had helped the DPRK evade sanctions and finance its nuclear weapons programme. This action prohibited financial institutions from maintaining correspondent accounts for or on behalf of Bank of Dandong, cutting the bank off from the US financial system. The designation also required financial institutions to apply special due diligence measures to guard against attempts by Bank of Dandong to access the US financial system.[2]

In the autumn of 2017, US and international sanctions increased as the DPRK regime continued to test nuclear weapons in the Korean peninsula.

On the same day it designated Bank of Dandong, FinCen also issued an advisory on North Korea's use of the international financial system.[3] The advisory described the complex manner in which the North Korean government used shell or proxy companies to evade US and international sanctions, and then provided a series of red flags of potential North Korean illicit financial activity. These red flags focused on geography (and China in particular), the use of Chinese aliases to operate companies in Liaoning province and in Hong Kong, the registration of multiple businesses or overlapping officers in these regions at the same address or phone numbers, the use of surge activity cycles, and involvement of particular industries such as textile, garment, and fisheries.

On 23 February 2018, the US Treasury's Office of Foreign Assets Control ('OFAC') took similar actions against a number of vessels, trading companies, and individuals that OFAC believed had helped North Korea evade sanctions through ship-to-ship petroleum transfers or concealed exports of North Korean coal. At the same time, OFAC issued a North Korean Sanctions Advisory on 'Sanctions Risks Related to North Korea's Shipping Practices'.[4]

This advisory described a series of measures that North Korean vessels had taken to evade sanctions, including physically altering vessel identifications, disabling or manipulating the automatic identification system ('AIS') data, and falsifying cargo and vessel documents. OFAC then recommended a series of risk mitigation measures for companies operating in the seas near the Korean peninsula. The OFAC announcement and advisory were accompanied by satellite photographs demonstrating some of these evasive tactics.[5]

More recently, in late July 2018, OFAC issued another enforcement advisory concerning the 'Risks for Businesses With Supply Chain Links to North Korea'.[6] This advisory illustrated a variety of techniques the North Korean government has used to evade sanctions, particularly with regard to the use of forced North Korean labour. As OFAC explained, it viewed the two primary risks as (1) inadvertent sourcing of goods, services, or technology from North Korea; and (2) the presence of North Korean citizens or nationals in companies' supply chains, whose labour generates revenue for the North Korean government. OFAC went on to describe in some detail how these practices work, and then outlined due diligence steps that companies should take to examine their entire supply chain for signs of illegal North Korean labourers or goods, and 'appropriate due diligence best practices' they should adopt, especially in high-risk countries and industries.

OFAC outlined due diligence steps that companies should take to examine their entire supply chain for signs of illegal North Korean labourers or goods.

Then again, on 3 August 2018, OFAC placed a Russian bank, Agrosoyuz Commercial Bank ('Agrosoyuz'), on the Specially Designated Nationals ('SDN') List for knowingly conducting or facilitating a significant transaction on behalf of North Korea's primary foreign exchange bank, Foreign Trade Bank ('FTB'). As OFAC explained in the designation announcement,[7] Agrosoyuz and North Korea had a 'long relationship', with the Russian bank processing millions of dollars in transactions for North Korean companies and front companies over the past decade.

On 15 August 2018, OFAC added Russian national Vasili Aleksandrovich Kolchanov, Dalian Sun Moon Star International Logistics Trading Co. Ltd. (Chinese company), SIN SMS Pte. Ltd. (Dalian Sun Moon's Singapore-based affiliate), and Profinet Pte. Ltd. (of which Mr. Kolchanov is the director general) to the SDN list based on purported violations of North Korean sanctions. OFAC announced that it was adding these parties because they were 'involved in facilitating illicit shipments on behalf of North Korea.' OFAC stated that the Dalien Sun Moon entities facilitated illicit shipments to North Korea, including exports of alcohol, tobacco and cigarette-related products, which provides the North Korean regime with over $1 billion in revenue. According to OFAC, Profinet, a Russian port service agency, and its director general, Kolchanov, provided port services to North Korean sanctioned vessels, including ones carrying refined oil products, in contravention of the oil-related sanctions on North Korea.[8]

Most recently, on 21 August 2018, OFAC added two new Russian entities and six Russian-flagged vessels to the SDN List for North Korea-related conduct. In particular, US officials determined that the entities owned and operated a vessel that was involved in ship-to-ship transfers of petroleum for the benefit of North Korea, an activity prohibited by the UN Security Council. Added to the US SDN List were Primorye Maritime Logistics Co. Ltd. and Gouzon Shipping Co. Ltd., as well as six vessels owned and managed by those entities.[9]

Enforcement goals

Viewed as a whole, these actions suggest that OFAC is devoting increased resources toward enforcement of the North Korean sanctions. The repeated and detailed guidance in this area, moreover, strongly indicates that OFAC has significant insight into how sanctions evasion is occurring, and is likely in the process of pursuing enforcement actions in this area. Based on this guidance, these enforcement actions likely involve the shipping industry, the fishing industry, the energy sector (oil, gas, and coal), the financial industry, and the textile and garment industries.

Companies working in these sectors, particularly in the East Asia region, should be on high alert for potential red flags, and should carefully review recent FinCen and OFAC guidance. Those advisories provide a host of compliance measures companies can adopt to ensure that they do not wind up in the next North Korean enforcement update.

Links and notes

1 https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13810.pdf

2 https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Financing%20Advisory%20FINAL%20111022017_0.pdf

3 https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf

4 https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/dprk_vessel_advisory_02232018.pdf

5 https://home.treasury.gov/news/press-releases/sm0297

6 https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf

7 https://home.treasury.gov/news/press-releases/sm454

8 https://home.treasury.gov/news/press-releases/sm458 and https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20180815.aspx

9 https://home.treasury.gov/news/press-releases/sm463

Tim O'Toole is a member of Miller & Chevalier Chartered in Washington, DC, where Claire Rickard Palmer is a senior international trade consultant.

totoole@milchev.com

cpalmer@milchev.com

Transit and the transport service providers – victims or facilitators?


Transport companies are the backbone of global supply chains, carrying our goods around the world. But should they be liable for compliance with export controls when often they are unaware of the true nature of the goods they are carrying, ask Gerard Kreijen and Martin Palmer with reference to recent Dutch enforcement actions.

International trade has developed in the last 50 or so years at a speed that has exceeded almost everyone's expectations. This growth, and ever-increasing security requirements, has driven the transport service providers ('TSPs') to innovate and develop creative and cost-effective solutions to their customers' increasing demands.

Very few transport companies are large enough to offer their own totally integrated service (door to door under their full control) and most rely on other service providers for elements of the international supply chain. Many transport companies, whilst offering their own transportation services are also filling the role of what is known as a 'freight forwarder' or 'forwarding agent'.

Freight forwarders bring together a wide variety of services and companies that together facilitate an international transaction between seller and buyer. These services utilise all modes of transport and often a single international transaction will involve movement by road, sea, air and rail. These services are not just related to the physical movement of a commodity but can also include packaging, documentation, customs export, transit and import processing, storage, licence processing and, in some transactions, acting as the exporter or importer of record. Trade facilitation expert, Dr Andrew Grainger's diagram (on the following page) demonstrates the complexity of the international supply chain and the different actors that may be involved in a single international transaction.

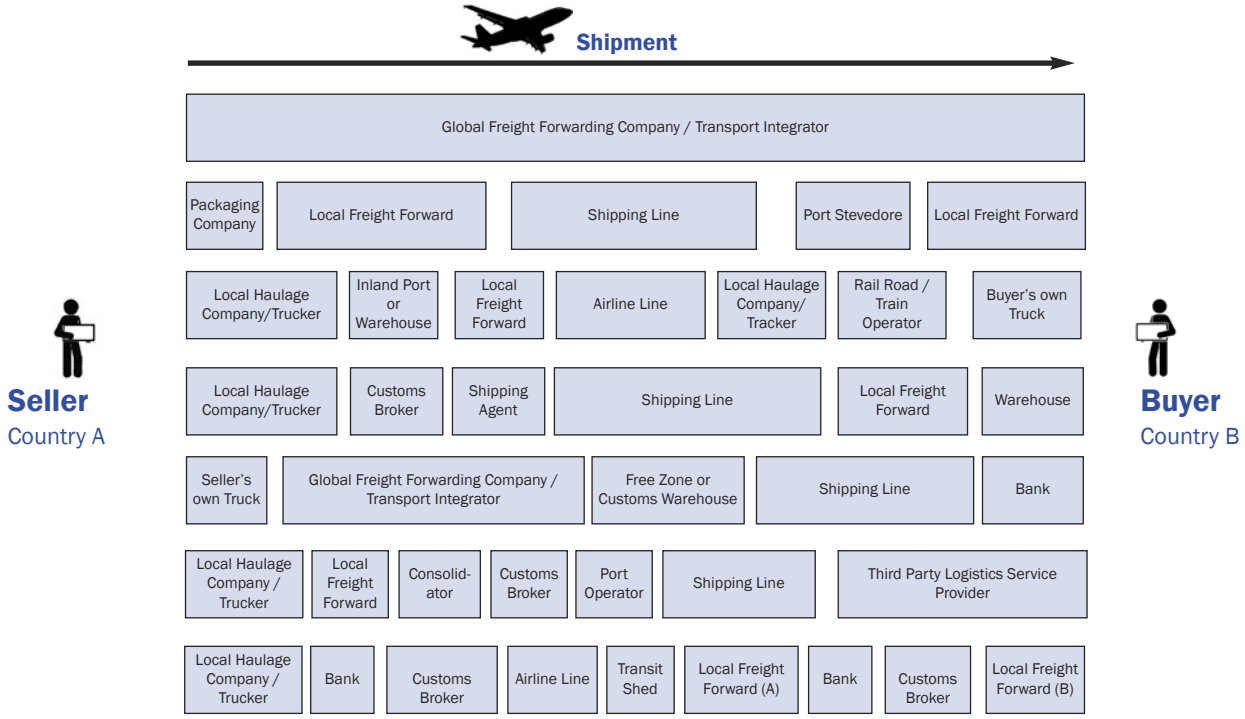
In Dr Grainger's example, the actors in the supply chain are individual companies, each completing a specialist transaction within the international movement. The seller and buyer will often be completely unaware of the individual actors and the part that they play. Likewise, the individual actors will be unaware of each other and will only be required to know the information that effects their part of the transaction. In the example of the transport service provider, this could be:

- Has the shipment been cleared for export?
- Does the shipment contain hazardous goods?
- Is the shipment correctly packaged?
- Do I have the necessary paperwork?

Often the TSP will receive from a freight forwarder a pallet or ULD[1] which will contain shipments from many different customers travelling to the same destination or for transhipment[2] at the next destination.

For shipments being directly exported or imported, the seller (consignor) or buyer (consignee), or a freight forwarder or forwarding agent acting on the seller's or buyer's behalf, will usually make a mandatory export declaration[3] to customs that includes information on the goods, consignor, and consignee.

For transiting or transhipping consignments, the information submitted to customs for control purposes may include a pre-arrival declaration or cargo manifest submitted by the carrier. The pre-arrival declaration or cargo manifest would consolidate information on all consignments carried but with significantly less information on each



Dr Andrew Grainger. Source: own practitioner observations; interviews

consignment compared to an associated export or import declaration. Consignments that transit or tranship are usually subject to significantly fewer regulatory and reporting requirements to facilitate trade because they are considered to pose limited, or no, fiscal, safety and/or security risks to the state through which they are passing. Since the seller and the buyer are unlikely to be established in the country of transit or transhipment, there will be limited or no additional information sources about them.

The freight forwarder may transport tens of millions of commodities on behalf of millions of customers each week. They do not own the commodities, nor do they have the technical knowledge of the commodities. They rely upon the data and documents provided by their customers. In the majority of cases, the customer of the TSP providing a service will be another TSP rather than the seller or buyer of the commodities, and the TSP will only have the information available to provide its element of the service.

The shortest distance between two points is a straight line. This is seldom the case in freight forwarding. The freight forwarder will often use the provider that provides the lowest cost whilst maintaining the service that the ultimate customer demands and the internal standards of the freight forwarder. Price is usually driven by available capacity on certain transport sectors. In many cases this is driven by the 'Hub and Spoke'[4] concept where an airline or TSP will set rates based upon spare capacity rather than distance travelled. Usually, the longer or further a shipment travels on a single journey the lower the cost will be. An example of this would be:

- A shipment from Barcelona, Spain to Oporto, Portugal.
  - The shortest route would be a direct flight on Iberia or TAP, Barcelona to Oporto;
  - The cheapest route, for example, could be a flight from Barcelona to Leipzig, transhipment to another aircraft, another flight from Leipzig to Lisbon, followed by a journey by road to a depot in Oporto where the shipment is loaded onto another smaller vehicle for locally delivery.

The ultimate routing of a shipment will often only be known to the TSP providing that element of the service.[5]

With TSPs actively encouraged by security authorities NOT to reveal the routings or timings of their networks, meaning, therefore, the seller is unaware of the countries in which the shipment may tranship, the seller's ability to know where a transit licence may be required is reduced. With the TSP taking responsibility for its part of the transaction only, based upon the limited amount of data provided by the previous actor, it can be difficult to see – certainly from a practical perspective – who has responsibility for acquiring a transit licence. (One should also consider that there are additional reasons that may influence a shipment's routing to its destination and these are often last minute and unforeseen. These can include rerouting due to weather or technical issues, off loads due to over capacity of aircraft, industrial (strike) action etc.)

The legal implications

This situation – where TSPs only receive limited information regarding the shipments they handle that concerns their part of the transaction, and sellers and buyers are generally unaware of the particular transits or transhipments of their goods – poses a considerable risk from an export controls perspective. This is particularly so if a shipment concerns

military goods, the transit or transhipment of which in principle requires a licence.

Three recent Dutch court cases vividly illustrate the risks that are involved.[6] A detailed discussion of these cases is beyond the scope of the present contribution, but it should be noted that each of the cases concerned the transit of military goods through Amsterdam airport and resulted in considerable fines. In two cases, logistic service providers were held liable for breaching applicable export control regulations. In the third case, the airline carrier was held liable.

In all three cases, the defendants had been charged with wilfully transiting listed military goods without a licence. In all of the cases, what strikes the eye is that the extensive scope of the applicable regulation in combination with the wilfulness criterion applied by the Dutch court, effectively resulted in a kind of strict liability for TSPs failing to obtain the required licence.

The scope of the applicable regulation

Under Dutch law,[7] the duty to request a licence rests on the person with the power of disposition, the person performing the customs formalities on its behalf or, if no customs formalities are being performed, the person transporting the goods. The Dutch court established that there is no order of precedence in this respect. Therefore, if several persons are (potentially) responsible for arranging a licence, the failure of one person to do so, will not discharge the others from their obligation. Needless to say, this puts at risk virtually any party involved in the handling of a shipment of strategic goods (logistic service providers, local freight forwarders, airline carriers, customs agents) for failing to obtain the required licences.

The wilfulness criterion

For a punishable transgression of an export control regulation to exist under Dutch law, the wilful intent of the transgression must be proven. Based on Dutch Supreme Court case law, a Dutch court will accept that a defendant wilfully transited or transhipped an item without the required licence if it merely executed the respective shipment. The wilfulness criterion is 'blanc', meaning that wilful intent is deemed to exist when directed at (the performance of) the prohibited act. Wilful intent to contravene the law (malicious or culpable intent) is not required for the wilfulness test to be met.

The duty to investigate

If one contrasts this risk with the developments in international trade – especially the limited transactional information on an international movement that will be normally available to the individual actors in the process – this raises the question as to whether it is fair to hold TSPs liable so easily. It should be noted that the parties most likely to have proper knowledge of the nature and destination of the goods – and hence, of any licensing requirements – are the seller and the buyer. Apart from the integrators that may be involved, most TSPs however, will have to rely on information which is summary at best, but which also may be incomplete, inaccurate or, even worse, false. Against this background, the virtual blanket liability the Dutch courts seem to have in store for the intermediate, actual handlers of the goods seems rather unfair. So is there, in effect, really some sort of strict liability for TSPs?

The extensive scope of the applicable regulation in combination with the wilfulness criterion applied by the Dutch court, effectively resulted in a kind of strict liability for TSPs failing to obtain the required licence.

On closer inspection, there is no strict liability in the sense that there is nothing that a TSP can do to escape criminal liability for transiting or transhipping military items without a licence. It is an established principle of Dutch criminal law that a crime shall not be punishable if there is an absence of (all) guilt on the part of the actor with respect to the unlawfulness of the act (or omission). Consequently, the three recent cases all deal with the defendant's 'duty to investigate', be it (with the benefit of hindsight) on a rather casual basis. The rationale for the court's inquiry into the defendants' duty to investigate is that if a defendant is able to show that it did everything reasonably possible to ascertain that it would be acting in compliance with applicable export control regulations, a breach would not be criminal and would go without punishment. However, in all three of the cases here, the court found, perhaps too easily, that the defendants had failed to meet their duty to investigate. This raises a legal and a practical question with which we will deal further below. Before doing so, however, here are some observations of the court with respect to the 'duty to investigate'.

In one case, a transit shipment of spare parts for Cheetah fighter jets from South Africa to Ecuador was intercepted by Amsterdam airport customs. The defendant (a Dutch airline carrier) had received the shipment from a logistics provider in South Africa. From the judgment, it follows that the master airway bill data – the transportation agreement between the TSP and the forwarder, here merely describing the goods as 'consolidation' – had given the company no cause to investigate the airway bills and the nature of the goods.

The judgment furthermore states that with respect to its deemed responsibility to apply for a transit licence, the defendant had argued that the logistics provider in South Africa was to be regarded as the (sole) person with the power of disposition. In this context, it had also argued that, based on the 1999 Montreal Convention, the logistics provider in South Africa, as the consignor of the goods, had a duty of care to provide adequate information on the goods that the shipment contained and was responsible for reporting to Dutch customs.

The court rejected these arguments quite bluntly, finding that the defendant, as the carrier of the goods, was to be regarded as a person having the power of disposition of the goods and, therefore, was under a duty to apply for the required transit licence. The court reiterated that, irrespective of whether or not the logistics provider had failed to comply with its obligations under the Montreal Convention, the defendant had its own responsibility and was therefore not

discharged from its duty to independently investigate with respect to the transit of strategic goods.

In a second case, in which judgment was rendered by the same court on the same day, checks by Amsterdam airport customs had shown that the goods that were being forwarded by the defendant (a logistics provider) actually were complete, military unmanned aircraft systems ('UAS' or drones) en route from the United States of America to Saudi Arabia. Having found that the defendant, as a logistics provider, qualified as a person having the power of disposition and, therefore, an obligation to have requested and obtained an individual transport licence, the court rejected the argument of the defendant that it did not know and had no reason to suspect that the shipment concerned military goods. The consignee (Saudi Arabia) and the description of the goods on the freight documents should have caused the defendant to investigate.

In this respect, the circumstances of the case showed that the defendant had already been issued with an official warning by the Dutch authorities concerning another shipment of (different) military goods that had also taken place without the required licence. At the time, the management of the company had undertaken to require the respective airway bill and invoice in addition to the usual 'OK to forward' from the foreign station in order to assess whether a shipment should be refused or a licence requested.

From a statement taken by customs it appeared that the defendant had received master airway bill data regarding the drones shipment which contained the description: 'PUMA AE II DDL' in addition to concise descriptions of origin and destination. The shipment had been offered to the defendant's Los Angeles station which had booked and listed it with an 'OK to forward' in the electronic freight forwarding message. Further inspection by customs, a report of which had been submitted to the court by the prosecution, had shown that the airway bill revealed the name and address of the US manufacturer/consignor and that the consignee was the 'Ministry of Defence, Royal Saudi Special Forces, Kingdom of Saudi Arabia' in Riyadh. The description of the goods on the airway bill stated: 'PUMA AE II-DDL SYSTEMS COMPLETE WITH ASSOCIATED ACCESSORIES AND TRAINING'.

The court considered that the defendant was not exculpated by the lack of information which it had received from its Los Angeles station, because the company had its own responsibility and was not released from its independent duty to investigate in matters concerning the transit of strategic goods. According to the court, this was all the more so because from the airway bills it was clear that the consignee was the Ministry of Defence of Saudi Arabia, while these also stated with respect to the nature of the goods that they concerned complete drones with associated accessories and training. This information should have given the defendant reason to further investigate, found the court.

The legal question

The first question raised by the court's observations with respect to the duty to investigate is a legal one. It asks: What is the scope of the duty to investigate under the particular facts and circumstances of the case? In short: What is the required standard of care the defendants should have applied in order to escape a penalty?

It seems reasonable, at first sight, to accept that the logistics provider in the drones case failed to investigate properly in light of the earlier warning it had received and its previous commitment to ask for the airway bill and invoice in addition to an 'OK to forward'. Here, the defendant itself had set a more or less clear standard which it subsequently failed to meet.

It is less easy to come up with a similar answer in the case of the airline company and the Cheetah fighter jet parts. Here, the defendant appears to have followed established procedures and there appear to be no immediate indications of a lack of diligence. It will be recalled that the master airway bill data only revealed South Africa and Ecuador as the origin and destination of the goods and that it only stated 'consolidation' as regards the type of goods. On the basis of this information, the defendant did not know that the consignor of the goods was Denel Aviation, a South African defence company, and that the consignee was the Ministry of Defence of Ecuador.

From a police report of an interrogation prepared by customs, it appeared that these additional details, according to the interrogated representative of the airline carrier, are normally contained in the house airway bill and the commercial invoice.

During the interrogation, the representative acknowledged that the airline carrier had its own duty to investigate. For this purpose, the company had its unit of experts tasked with assessing possible licensing requirements for shipments on the basis of the airway bills and ancillary documents. Because of the large numbers of shipments, however, the instruction was not to ask for the underlying paperwork of all consolidations. The information contained in the master airway bill data of this shipment had not given cause for inspection of the airway bill and the house airway bill before unloading at Amsterdam airport.

In finding that the defendant had its own duty to independently investigate, the court seems to have relied heavily on the customs police report which did contain details on the origin and final destination of the goods from the house airway bill. Thereby the court effectively ignored the defendant's explanation that it had in place and followed quite detailed procedures which had raised no flags on the basis of the master airway bill data.

It is essential to develop a solution that is capable of pinpointing the military nature of a good upon entry of the supply chain.

It seems open to debate, therefore, whether or not the defendant under the facts and circumstances of the case indeed fell short of the applicable standard of care (which was never elaborated by the court). As a matter of fact, the judgment in the third case – and also that in the second case, if we ignore the earlier warning issued to the logistics provider – follows a similar pattern. Further clarification is required and it would seem that this is the reason an appeal against the judgment in the first and third case is currently pending.[8]

The practical question

The second question is the more difficult one and it is, at any rate, the more important one for TSPs. It is of a practical nature. Assuming that TSPs have a general duty to investigate, how can this duty be reconciled with their business models and the features of modern international trade as set out above? To say that TSPs will simply have to follow suit if they want to escape liability is to ignore the practical difficulties, including the potentially far-reaching commercial consequences, they are facing. How does one establish the need for a particular transit licence if there are thousands of shipments on a daily basis, where routing may be uncertain until moments before dispatch (or even thereafter), and there is only scanty information on the nature and the destination of the goods?

Reviewing individual airway bills and invoices, even if theoretically possible, is a practical nightmare given the numbers involved. It raises great difficulties from the perspective of capacity and timing and is likely to result in delays. Because of small margins and fierce competition, it is also commercially self-defeating.

A first step to deal with this seemingly insurmountable problem may be to bring down numbers by focusing on and selecting shipments that hold the potential of an increased risk. A practically feasible approach to filter such shipments from the vast daily totals could be to ask the questions, 'Who?', 'What?' and 'Where/to whom?' (in that order).

The 'Who?' question would be KYC-like. TSPs will know many of their regular customers and the kind of business they are in. Such regular customers obviously pose no risk if they are not in the business of trading in

Links and notes

[1] A 'unit load device' (ULD) is a pallet or container used to load luggage, freight, and mail on wide-body aircraft and specific narrow-body aircraft. It allows a large quantity of cargo to be bundled into a single unit. Each ULD has its own packing list (or manifest) so that its contents can be tracked.

[2] 'Transit' is the transport of goods through a territory where the goods remain on board the original means of transport (e.g., vessel, train or aircraft). 'Transhipment' is the transport of goods through a territory where the goods are unloaded from one means of transport and loaded on to another means of transport (e.g., from a vessel to a train, from an aircraft to another aircraft etc.).

[3] Data requirements for shipments transported by postal organisations are usually significantly less than those required by the private sector.

[4] A 'Hub-and-Spoke' network is a network in which all nodes are connected to one central node, which acts as the hub. This is the system used by most legacy carriers around the world. For example, if you would fly from Hong Kong to Glasgow, you would most probably fly to a European hub such as Amsterdam or London Heathrow and then take another flight on a smaller aircraft to Glasgow.

[5] This is not uncommon and since the terrorist bombing of Pan Am Flight 103, over Lockerbie, Scotland in December 1988, TSPs have been actively encouraged not to reveal the routings of shipments within their networks. Pan Am 103 was a regular scheduled transatlantic flight from Frankfurt to Detroit via London and New York. The explosive device actually originated at Luga Airport, Malta. The terrorists, knowing the routing, trans-shipment points, airlines and timing of flights were able to select a location to onboard the bomb that would attract the least amount of suspicion and set the timer on the device to explode over the North Atlantic, based upon the schedule timings. This was executed perfectly and, but for a departure delay at London Heathrow, Pan Am 103 would have exploded over the North Atlantic along with all of the evidence.

[6] See North Holland District Court (Rechtbank Noord Holland) cases no. 15/994176-17 of 24 April 2017, summarised and briefly discussed at: http://www.worldtradecontrols.com/export-controls-enforcement-by-the-dutch-court-part-1-the-case-of-the-logistics-provider/; 15/994178-17 of 24 April 2017, summarised and briefly discussed at: http://www.worldtradecontrols.com/export-controls-enforcement-by-the-dutch-court-part-2-the-case-of-the-airline-company/; Amsterdam District Court (Rechtbank Amsterdam) case no. 13/994046-17 of 23 November 2017, summarised and briefly discussed at: http://www.worldtradecontrols.com/shipping-criminal-liability-the-difficult-position-of-the-transportation-logistics-sector/.

[7] Article 3 of the 2012 Dutch Implementation Regulation Strategic Goods (*Uitvoeringsregeling strategische goederen* 2012).

[8] Although the discussion of the possible legal implications for postal shipments is beyond the scope of the present contribution, a few general observations in this respect may be added. TSPs often transport shipments for postal authorities which have much lower data requirements and simplified export, transit and import declarations. Moreover, contrary to consolidated air freight, the transport documentation of postal shipments will generally not reveal anything about the possible military nature of the shipped items. Such postal transport documents will refer to the respective 'mailbag' and simply state 'letters' or 'parcels'. Ignoring for the moment that the specific regulatory framework for postal shipments may result in different liabilities for export control violations, it is possible to draw two general conclusions for postal shipments from the reasoning applied by the Dutch court. First, based on the extensive scope of the applicable regulation and the 'blanc' wilfulness criterion, TSPs would in principle also be liable for transiting or transhipping a postal item without the required licence. Secondly, it would seem that in the case of postal shipments TSPs are in a better position to rely successfully on an 'absence of all guilt' defence and escape penalties simply because they do not have at their disposal the required information that would enable them to investigate whether or not they are shipping a military good.

[9] In this respect it should not be ignored, however, that in many cases TSPs do not accept individual transactions but take consolidated shipments, physically consisting of ULDs onto which large quantities of cargo have been bundled. An in-depth review of this practical complication is beyond the scope of the present contribution, but any proposal for effectively dealing with the overall problem will eventually have to face it. Nevertheless, with regard to these consolidated transactions, it would seem that a general requirement in the terms of trade obliging sellers to flag the military or controlled nature of an item could be part of a practically workable procedure.

strategic goods. And these customers are likely to constitute a not-insignificant part of the client base of any TSP at any time. Many TSPs, of course, have 'unknown shipper' policies, which require further data before transport and which they apply as a self-managed standard. Eventually, such policies will only be effective if they properly address and require a satisfactory answer to the 'What?' question below.

The 'What?' question, to be addressed to the non-regular customers, would be aimed at establishing whether the goods to be moved could be military. The vast majority of the goods are unlikely to classify as military goods. The 'What?' question may be subject to the consideration that in order to avoid requiring an answer regarding all transactions (causing delays in light of the sheer volume) it may be more practical to include in the terms and conditions of trade the need for military or controlled goods to be flagged by the contracting party.

The 'Where/to whom?' question should provide greater clarity about the potential risk of shipments to sanctioned destinations and end-users, but at the same time it could provide useful clues in combination with the determination of the military nature of the goods on the basis of the 'What?' question. At any rate, it is a must to ask the third question if a shipment is known to be military.

Admittedly, the above sequence of questions is hardly the practically efficient overall solution that TSPs will require. It should be seen as a first step of a move to control existing risk. As such, however, this approach cannot evade the basic problem that the customer offering the goods often will not be the seller, but another TSP acting on poor information regarding the origin, destination, and nature of the items in transit. Integrators, perhaps, are in a position to ask these questions and receive satisfactory answers, but most TSPs are not.

The heart of the matter is that once a military item has entered the supply chain undetected, TSPs will have difficulties obtaining the information enabling them to clarify the applicable licensing requirements, even if they are keen to do so.

It is essential, therefore, to develop a solution that is capable of pinpointing the military nature of a good upon entry of the supply chain and that, in the event of a positive determination, is designed to convey that information, for example as part of the master airway bill data, to any down-chain intermediate party accepting the shipment. It really is the (military) nature of the good that triggers the risk of criminal liability if it goes unnoticed.

The cardinal question, therefore, is whether practically feasible measures can be taken to ensure easy identification of military goods upon entry to the supply chain and how to pass on the relevant information. Given the number of potential parties involved in the movements of a shipment (sellers, integrators, other intermediate TSPs, buyers) any satisfactory solution seems to hinge on a cooperative effort that is based on mutual self-interest. Naturally, the parties dealing directly with the sellers are in the best position to determine the military nature of a good, simply by asking the question when being offered the shipment.[9] It seems practical and reasonable that they should bear principal responsibility in this respect. But the responsibility of the intermediate TSPs is not a lesser one, since identification upon entry of the supply chain becomes pointless if it is not consistently shared with additional recipients upon transfer from one TSP to another.

That being said, it should not be overlooked that the perfect compliance policy simply does not exist. In the event of a breach, therefore, the main question in court (at least in a Dutch court) will not be whether the defendant TSP had in place a state-of-the art policy whereby any military goods could have been spotted and tracked at any time, but rather whether it took reasonable measures in light of the facts and circumstances to prevent the breach. In other words, even if there is no waterproof compliance procedure, a defendant may still be able to show that it has exercised the required diligence to avoid violation and escape a penalty. For the moment, however, the difficulty is that Dutch case law gives no useful guidance on the level of diligence that TSPs are supposed to exercise when investigating shipments for possible licensing requirements.

Gerard Kreijen is Counsel at Loyens & Loeff N.V. He is based in Amsterdam and co-heads the Loyens & Loeff International Trade team. Martin Palmer is the founding partner of Supply Chain Compliance Ltd and Chief Content and Compliance Officer for Hurricane Modular Commerce Ltd.

gerard.kreijen@loyensloeff.com
martin.palmer@supplychaincompliance.net

US sanctions and export controls: What every healthcare and life sciences compliance officer needs to know




Ama Adams, Laura Hoey, Brendan Hanifin and Emerson Siegle provide a seven-point check-up for healthcare and life sciences companies seeking a compliance clean bill of health.

The economic sanctions and export compliance challenges facing healthcare and life sciences companies have never been more acute. Many companies have established comprehensive policies, procedures, and controls to promote compliance with the US Food and Drug Administration ('FDA') and Department of Health and Human Services regulations, as well as to deter violations of fraud and abuse laws, the False Claims Act, and the Foreign Corrupt Practices Act. Fewer healthcare and life sciences companies have devoted similar attention and resources to developing robust economic sanctions and export compliance programmes, notwithstanding the US government's escalating enforcement of these laws.[1]

This article discusses seven significant sanctions and export compliance risks facing healthcare and life sciences companies, drawing upon the most frequent questions we receive from industry compliance personnel.

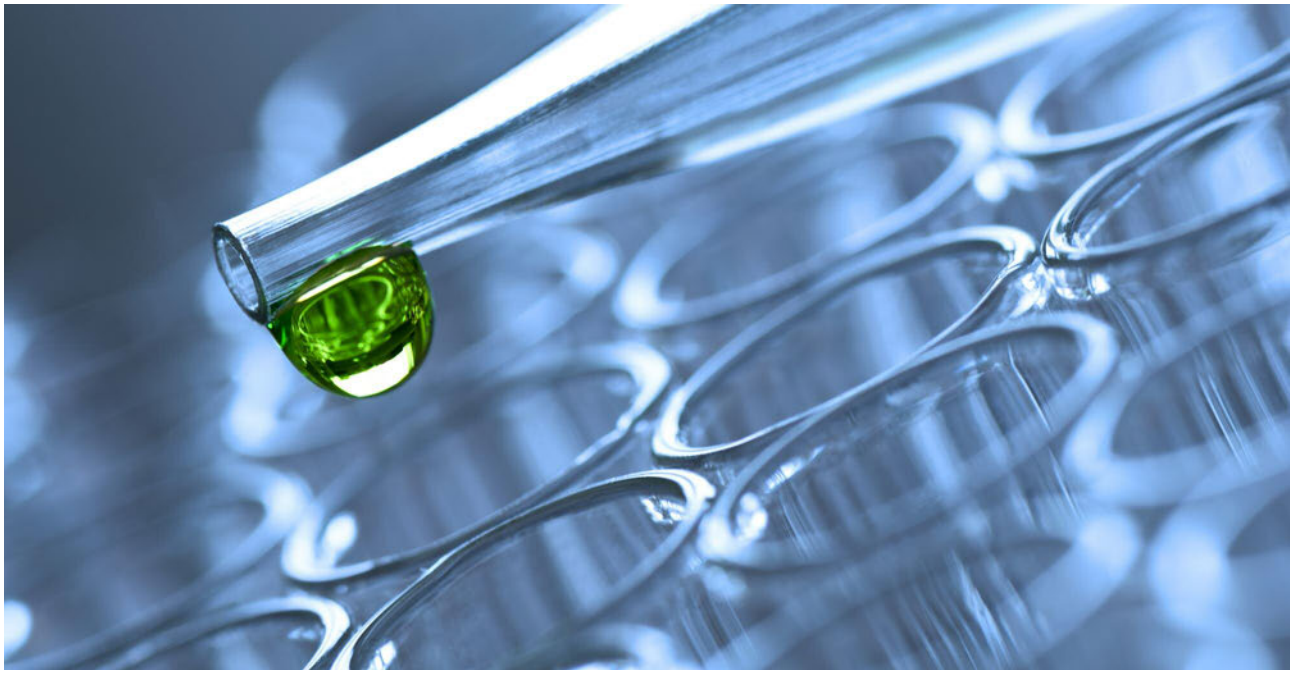
1) US sanctions and export controls have broad extraterritorial application

Frequently, employees of healthcare and life sciences companies – whether employed within or outside of the United States – do not appreciate the broad extraterritorial reach of US sanctions and export control laws. US sanctions and export control laws can regulate conduct that (1) occurs entirely outside of the United States; and (2) does not involve US citizens or companies. As such, healthcare and life sciences companies, whether organised in the United States or another jurisdiction, cannot necessarily rely upon the absence of a clear or logical nexus with the United States to insulate their operations from potential scrutiny.

US sanctions generally apply to 'US persons', which include (1) US citizens and permanent resident aliens, wherever they are located in the world; (2) entities organised under US law (including overseas branch or representative offices); and (3) any person physically located within the United States, regardless of nationality.

The United States' Cuban and Iranian sanctions programmes also apply to entities that are 'owned or controlled' by US persons – namely, non-US entities in which a US person (1) holds a 50% or greater equity interest by vote or value; (2) holds a majority of board seats; or (3) otherwise controls the actions, policies, or personnel decisions of the entity.[2]

In addition, the United States



maintains 'secondary sanctions' that specifically target non-US persons, ordinarily outside of OFAC's jurisdiction, who engage in certain dealings with Iran, North Korea, or Russia.

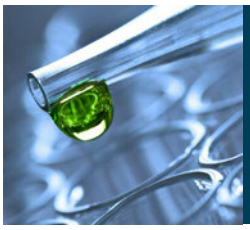
The Export Administration Regulations ('EAR') – the primary US export control regime relevant to healthcare and life sciences companies – regulate 'US-origin items', as opposed to specified classes of individuals or entities.[3] Items subject to the EAR include (1) US-origin items, wherever located; (2) US-origin parts, components, materials, or other commodities incorporated abroad into foreign-made products; (3) certain foreign-made direct products of US-origin technology or software; and (4) items physically located in the United States, regardless of origin.[4] Because the EAR regulate the disclosure of controlled technology to foreign nationals, even US companies with 'exclusively' domestic operations must consider export compliance in connection with (1) the hiring of foreign national employees or contractors; and (2) interactions with foreign national counterparties, such as customers or suppliers.

Identifying where a company's operations could implicate US sanctions or export control laws frequently requires collaboration across key functional areas, including compliance, legal, finance, logistics, and procurement. While there is no one-size-fits-all compliance model, effective sanctions and export compliance programmes typically employ a combination of automated or semi-automated controls (e.g., counterparty screening, embargoed country blocks, new vendor and customer on-boarding requirements) with proactive compliance steps (e.g., employee education, regular compliance communications, and periodic risk assessments).

2) Export-controlled products and technology may not be obvious

While healthcare and life sciences products frequently are perceived as therapeutic (or, at worst, benign), many products and technology common to the industry are subject to US export control restrictions or licensing requirements. For example, certain biological materials (including certain human, animal and plant pathogens; toxins; genetically modified organisms; vaccines; medical products (e.g., certain devices and component parts); and diagnostic and food-testing kits, as well as certain chemicals and biomedical and chemical-handling equipment (e.g., storage tanks; reactors; pumps; and valves) may require a licence for export depending on the destination or end-user.[5] Failure to identify controlled items or technology and to comply with country-specific licensing requirements may result in significant fines, imprisonment for individuals, or even loss of export privileges (a putative death penalty for many companies).

Healthcare and life sciences companies should consider establishing formal procedures for the classification of products, equipment, and technology. Companies that lack the technical expertise to perform export classifications in-house may consider (1) seeking formal classification determinations from the Bureau of Industry and Security ('BIS') or the US State Department, as applicable; or (2) engaging outside counsel or a consultant to perform vendor-assisted classifications.



Healthcare and life sciences companies should consider establishing formal procedures for the classification of products, equipment, and technology.

3) It is surprisingly easy to commit unlawful facilitation of a prohibited transaction

OFAC sanctions prohibit US persons – including US citizens, wherever they are located in the world – from facilitating transactions involving sanctioned parties or embargoed countries, if the underlying transaction would be prohibited if executed directly by a US person.[6] US-organised companies, as well as companies that employ US citizens (as directors or as employees), should take care that US citizens do not participate in, or facilitate, transactions involving sanctioned parties or embargoed countries. Importantly, the restriction against US citizens' facilitation of transactions involving sanctioned parties or embargoed countries generally applies even if a US citizen's employer is a non-US entity (and therefore generally not required to comply with US sanctions).

Healthcare and life sciences companies subject to US jurisdiction cannot refer business involving sanctioned parties or embargoed countries to parties located outside of the United States (e.g., subsidiaries or distributors). Potentially problematic referrals typically arise in one of two scenarios, illustrated by the following examples:

Example 1: A US-based customer service representative is contacted by a Belgian distributor regarding a purchase order for an end-user located in North Korea. The customer service representative determines that her employer cannot lawfully export the requested products or services, directly or indirectly, from the United States to North Korea. The customer service representative therefore directs the distributor to contact a customer service colleague based in her company's Asia regional headquarters, located in China.

Example 2: An employee of a German company, which is majority owned by a US private equity firm, is contacted regarding a potential business opportunity in Iran. After determining that his employer cannot lawfully pursue the opportunity, the German employee refers the opportunity to another German company that is not owned or controlled by a US firm.

Employee education – imparted through clear policies and targeted training for relevant personnel – is the most effective way to prevent impermissible facilitation of transactions involving sanctioned parties or embargoed countries. In addition, healthcare and life sciences companies subject to US jurisdiction should consider whether their policies or reporting lines, or the organisation of their back-office support functions

(e.g., accounting, information technology), present unnecessary facilitation risk.

4) All licences are not created equal

US sanctions regulations and export control laws provide for various general licences and other exceptions that authorise certain transactions that otherwise would be prohibited. In addition, OFAC and BIS each may issue specific licences that authorise transactions – typically, limited by time, quantity, end-user, and product type – that do not fit within the scope of an existing general licence or exception.

Relevant to healthcare and life sciences companies, OFAC has issued general licences that authorise donations of food and medicines, as well as exports of certain medicines and medical devices, to embargoed countries. However, the scope of these general licences is limited (and is not necessarily consistent from country to country). For example, OFAC has issued a general licence authorising US persons to participate in joint medical research projects with Cuban nationals and to engage in certain interactions with the FDA in connection with Cuban-origin pharmaceuticals.[7] However, the Cuban sanctions specify that other medical research or transactions involving pharmaceutical products not explicitly authorised by the general licence are prohibited.[8] BIS abides by a general policy of denial with respect to exports or re-exports of items subject to the EAR to comprehensively sanctioned jurisdictions. Like OFAC, however, BIS recognises limited exceptions with respect to exports of medicines and medical devices. For example, a licence is not required to export or re-export to North Korea medicine designated as EAR99, although a licence is required to export or re-export to North Korea medicine on the Commerce Control List, such as certain vaccines and immunotoxins, and medical devices that are subject to the EAR.[9] Similarly, BIS has adopted a general policy of approval with respect to exports and re-exports of medicines and medical devices (whether sold or donated) to Cuba, though (unlike North Korea) a would-be exporter would still need to apply for the licence.[10]

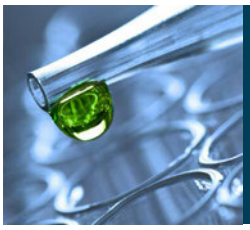
Given that OFAC and BIS licences vary in scope, and are updated from time to time, healthcare and life sciences companies should consider vetting with qualified counsel any transactions that are intended to be executed pursuant to a license or other regulatory exception.

5) You may need a map and a lawyer to navigate the Iran sanctions

In May 2018, the United States announced its withdrawal from the Iran nuclear deal, the Joint Comprehensive Plan of Action ('JCPOA'), as well as the re-imposition of sanctions targeting Iran following a 90-day or 180-day wind-down period. On 27 June, OFAC revoked General License H, which allowed foreign-organised companies owned or controlled by US persons to engage in certain dealings with Iran. On the same day, OFAC issued a new general licence authorising transactions and activities ordinarily incident and necessary to the wind down of transactions previously authorised under General License H. As a result, healthcare and life sciences companies that were previously conducting business with Iran pursuant to General License H must ensure that all such activities are completed by 4 November 2018.

Prior to 27 June, some non-US healthcare and life sciences companies conducted business with Iran in 'partial reliance' on General License H. Such companies have minority US investors who may – or may not – exercise 'control' over the company's actions, policies, or personnel decisions. Following the revocation of General License H, if they wish to continue conducting business with Iran, these companies must (1) make an at-risk determination they are not controlled by their US investors; or (2) identify a separate OFAC authorisation (e.g., the medicines and medical devices general licence, discussed below) for their Iran-related dealings.

Similar to other country sanctions programmes, OFAC has issued a general licence authorising the export and re-export of certain medicines and medical devices to Iran.[11] This general licence has been in effect since 2011, and there is no indication that OFAC intends to revoke or modify the licence in connection with the United States' withdrawal from the JCPOA. Importantly, the general licence is subject to several limitations. First, the general licence does not cover certain categories of medicines and medical devices (e.g., cholinergics, opiods, narcotics, benzodiazapenes, etc.).[12] Second, the general licence excludes certain categories of end-users, namely Iranian military, intelligence, or law enforcement purchasers and specially designated nationals ('SDNs').[13] Third, exports or re-exports of covered medicines or medical devices must be shipped within 12 months of signing the underlying contract for the provision of such products.[14] Fourth, transactions executed pursuant to the general licence must comply with certain, specified payment terms (i.e., payment of cash in advance, sales on open account, financing by third-country financial institutions, or certain letters of credit).[15]



OFAC has issued general licences that authorise donations of food and medicines, as well as exports of certain medicines and medical devices, to embargoed countries.

Finally, certain aspects of the Iran sanctions apply to non-US individual and entities, who are not generally subject to OFAC's jurisdiction. For example, non-US persons are prohibited from (1) exporting US-origin products or services to Iran; or (2) causing another party to violate the Iranian sanctions, such as by causing an Iran-related payment to be processed via a correspondent account in the United States or at a foreign branch of a US bank. In addition, secondary sanctions may attach to non-US persons' dealings with sanctioned Iranian parties, the Islamic Revolutionary Guard Corps ('IRGC') and its designated agents or affiliates and, in connection with the United States' withdrawal from the JCPOA, critical Iranian industries (such as Iran's shipping, energy, and financial sectors). As a result, non-US individuals and entities should exercise

caution – and, at minimum, perform appropriate due diligence – in connection with Iran-related transactions.

6) Fair or not, you may be liable for your third-party agent's conduct

Many healthcare and life sciences companies rely upon third parties, such as distributors, dealers, sales agents, or resellers, to market and sell their products throughout the world, including in countries subject to sanctions and export controls. Engagement of third-party intermediaries presents various sanctions- and export compliance-related risks, including that (1) the intermediary may resell products to sanctioned parties or embargoed countries, or in violation of US export control laws; or (2) the intermediary itself – or its owners – may be targeted by sanctions or export restrictions.

Contract research organisations ('CROs') often reduce costs for healthcare and life science companies developing new medicines and medical devices in foreign markets. However, while CROs can offer significant logistics-related efficiencies and cost savings, reliance on these third parties does not necessarily mitigate sanctions and export control risk. Frequently, the healthcare and life sciences company will remain legally responsible for complying with US export control laws, even if day-to-day management is delegated to a CRO (or customs broker, freight forwarder, or other third-party intermediary). Reliance on CROs may present other risks as well. For example, sharing of information with CROs or foreign employees of CROs can constitute an export (and potentially require a licence, even if the exporter and CRO are under contract). As a general matter, healthcare and life sciences companies should conduct the same, risk-based due diligence and ongoing monitoring of CROs as they would of other third parties, in addition to seeking appropriate contractual protections.

OFAC and BIS have brought multiple enforcement actions against US companies based on the conduct of third-party intermediaries. Historically, such enforcement actions have been premised on the knowledge (actual or constructive) of the underlying violations by a party subject to US jurisdiction. However, in a recent enforcement action involving a non-healthcare or life sciences company, OFAC imposed a multi-million-dollar penalty, despite being unable to prove that the company's products actually were re-exported to an embargoed jurisdiction.

In 2014, OFAC penalised Epsilon Electronics, a US-based audio electronics company, $4,073,000 for exporting products to Iran via a reseller located in the United Arab Emirates. Though it could not prove that the Dubai-based reseller had re-exported Epsilon's products to Iran, OFAC concluded that Epsilon had reason to know that its products would be re-exported to Iran based, *inter alia*, on information on the reseller's website. Epsilon challenged OFAC's penalty, but OFAC prevailed at both the district court level and on appeal.[16]

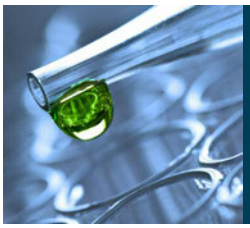
The Epsilon case underscores the importance of conducting pre-engagement due diligence and ongoing monitoring of third-party intermediaries, to ensure that third parties' activities will not potentially expose healthcare and life sciences companies to sanctions or export control liability. In particular, companies must remain vigilant of potential red flags suggesting that third-party intermediaries have, or intend to, divert their products to a restricted destination or end-user.

Companies may seek further protection by negotiating third-party agreements that incorporate robust sanctions and export compliance representations and warranties, as well as periodic or 'for cause' audit rights (as commercially feasible).

Finally, healthcare and life sciences companies should consider seeking periodic certifications of compliance with relevant sanctions and export control laws from third-party intermediaries.

7) You don't need to ship anything to run afoul of export control laws

US export control laws regulate the 'release' of controlled technology, source code, software, or technical data to foreign nationals (whether located within or outside of the United States). Such a release is *deemed* to be an export to the home country of the foreign national. Healthcare and life sciences companies may contend with deemed export risk – for example, in connection with (1) hiring of foreign national employees or contractors; (2) site visits by foreign nationals (e.g., prospective customers or suppliers); or (3) engagement in research collaborations with institutions located outside the United States or that employ foreign nationals (e.g., visiting scholars).



Companies should consider seeking periodic certifications of compliance with relevant sanctions and export control laws from third-party intermediaries.

To mitigate the risk of inadvertent export control violations, healthcare and life sciences companies should consider implementing formal protocols for addressing situations that may result in the release or disclosure of controlled US technology to a foreign national. Such protocols, often referred to as 'technology control plans', may include, *inter alia*, (1) procedures for screening and pre-clearing foreign national employee candidates before they are permitted to access controlled information; and (2) requirements to obtain appropriate export compliance-related representations and warranties from counterparties to research collaboration agreements.

The risks are real

In 2017, OFAC announced two enforcement actions targeting healthcare and life sciences companies (one of the companies also was the subject of a BIS enforcement action in 2013). Although the penalties imposed in these actions were modest by OFAC standards, in recent years, OFAC and BIS have imposed multi-million-dollar penalties against US and non-US companies.

In February 2017, United Medical Instruments ('UMI') agreed to pay $515,400 to resolve 56 alleged violations of the Iran sanctions.[17] OFAC alleged that, between December 2007

and April 2009, UMI made sales of medical imaging equipment with knowledge or reason to know that the goods were intended specifically for supply or re-exportation to Iranian buyers. The total value of the medical equipment at issue was nearly $2.5 million, and the maximum statutory penalty for UMI's alleged violations was over $10 million. In determining the settlement amount, OFAC took into account several mitigating factors, including UMI's small size and remedial efforts, as well as the company's cooperation with OFAC's investigation

In December 2017, DENTSPLY SIRONA Inc. ('DSI'), agreed to pay $1,220,400 to resolve 37 alleged violations of the Iranian sanctions.[18] Between November 2009 and July 2012, DSI subsidiaries exported 37 shipments of dental equipment and supplies from the United States to distributors in third countries, with knowledge or reason to know that the goods were ultimately destined for Iran. OFAC calculated a statutory maximum penalty of $9,551,082 and, as in the UMI settlement, identified several mitigating factors (including that the exports at issue likely were eligible for a specific licence). According to the enforcement information, DSI agreed to toll the statute of limitations for over three years (1,104 days), demonstrating that OFAC enforcement actions can take years to resolve and may impose significant costs (e.g., legal fees, management distraction) in addition to monetary penalties.

Recent developments in US sanctions have been occurring at an unprecedented pace (and which shows no signs of abating). And while less publicised, the Commerce and State departments have continued to push ahead with the US government's export control reform initiative by reclassifying less sensitive items from the US Munitions List to the Commerce Control List. The pace of change puts enormous pressure on in-house legal and compliance professionals.

In light of escalating enforcement of economic sanctions and export control laws, it is incumbent upon healthcare and life sciences companies to invest in compliance and to assess carefully the risks and benefits of engaging in business that could potentially violate applicable laws.

Links and notes

[1] This article focuses on compliance with US law because, as a practical matter, the United States is the most rigorous enforcer of its sanctions and export compliance regimes. However, multinational companies also are subject to the sanctions and export control laws of other jurisdictions in which they operate.

[2] The US Department of the Treasury's Office of Foreign Assets Control ('OFAC'), the agency responsible for administering and enforcing US sanctions, has issued limited guidance regarding the scope of the third, 'control' prong of the 'owned or controlled' standard. As a result, non-US companies that are minority owned by US persons sometimes must pursue or forego potentially lucrative opportunities based on an imprecise standard. 31 C.F.R. § 515.329; 31 C.F.R. § 560.215.

[3] The International Traffic in Arms Regulations control certain chemical and biological agents, as well as equipment used to handle or dispose of such agents.

[4] 15 C.F.R. § 734.3

[5] Of note, publicly available technology that would ordinarily require a licence for export to certain destinations does not require a licence if it has been published and is generally accessible to the interested public (e.g., published in a scientific journal), or if it arises from 'fundamental research' – both basic and applied – where it ordinarily would be widely shared within the scientific community.

[6] Facilitation is a loosely defined concept – whose technical definition varies across US sanctions programmes – leaving US persons (and their legal advisors) precious little guidance from which to assess the risks presented by proposed transactions or activities. On one end of the spectrum, approving, financing, or guaranteeing transactions involving sanctioned parties or embargoed countries – absent an applicable licence or exception – clearly is prohibited. See, e.g., 31 C.F.R. § 560.208. On the other end of the spectrum, '[a]ctivity of a purely clerical or reporting nature that does not further trade or financial transactions' with sanctioned parties or embargoed countries may not violate US sanctions. 31 C.F.R. § 538.407 (repealed 2017).

[7] 31 C.F.R. § 515.547(a).

[8] Id. § 515.547(e)(2)

[9] See North Korea, https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/north-korea.

[10] See Cuba, https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/cuba.

[11] 31 C.F.R. § 560.530

[12] Id. § 560.530(a)(3)(ii), (iii). Since 2016, certain healthcare and life sciences companies whose products are outside the scope of the medicines and medical devices general licence have conducted business with Iran pursuant to General License H. As General License H has now been revoked, these companies must (1) wind down their Iranian sales by 4 November 2018; or (2) seek specific authorisation from OFAC to continue their sales to Iran.

[13] Id. § 560.530(a)(3)(iv)

[14] Id. § 560.530(a)(3)(i)

[15] Id. § 560.532

[16] *Epsilon Elecs. v. US Dep't of Treasury, Office of Foreign Assets Control*, 857 F.3d 913 (D.C. Cir. 2017).

[17] OFAC, United Medical Instruments Inc. Settles Potential Civil Liability for Alleged Violations of the Iranian Transactions and Sanctions Regulations (Feb. 28, 2017), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20170228_united_medical_technologies.pdf. According to the Enforcement Information, UMI's obligation to pay the settlement amount would be deemed satisfied by the company's compliance with the terms of a 2013 settlement with BIS and payment of $15,400 to OFAC.

[18] OFAC, DENTSPLY SIRONA Inc. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations (Dec. 6, 2017), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20171206_Dentsply.pdf.

Ama Adams and Laura Hoey are partners at US law firm Ropes & Gray, where Brendan Hanifin is counsel and Emerson Siegle is an associate.

Ama.Adams@ropesgray.com
Laura.Hoey@ropesgray.com
Brendan.Hanifin@ropesgray.com
Emerson.Siegle@ropesgray.com

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Julia Bell, Deloitte
www2.deloitte.com

Dr. Scott Jones, TradeSecure, LLC
http://tradesecure.net/

Tim O'Toole and Claire Rickard Palmer,
Miller & Chevalier Chartered
www.millerchevalier.com

Barbara Linney, Miller & Chevalier Chartered
www.millerchevalier.com

Gerard Kreijen, Loyens & Loeff N.V. and Martin Palmer,
Supply Chain Compliance Ltd
www.loyensloeff.com / www.supplychaincompliance.net

Ama Adams, Laura Hoey, Brendan Hanifin and
Emerson Siegle, Ropes & Gray
www.ropesgray.com

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 [0072]

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 72. SEPTEMBER 2018
www.WorldECR.com