WorldECR

ISSUE 52. JULY/AUGUST 2016
www.WorldECR.com

Canada introduces new controlled exports smuggling offence

On 15 June 2016, the government of Canada introduced Bill C-21, 'An Act to amend the Customs Act' in the House of Commons. The amendments to the Customs Act focus on exports of people and goods. Many of the amendments deal with the gathering of information about the export of goods and people. According to Cyndee Todgham Cherniak of Toronto's LexSage, one of the hidden changes relating to export smuggling may be especially important for businesses.

New subsection 159(2) of the Customs Act creates a new offence of smuggling out of Canada.

Todgham Cherniak says that new subsection 159(2) of the Customs Act creates a new offence of smuggling out of Canada. It provides: 'Every person commits an offence who smuggles or attempts to smuggle out of Canada, whether clandestinely or not, any goods that are subject to duties, or any goods the exportation of which is prohibited, controlled or regulated under this or any other Act of Parliament.'

Todgham Cherniak says the provision must be read in conjunction with a number of other statutes. She adds, 'Section 160 of the Customs Act is amended to extend the punishment to export smugglers. If a person commits an offence under new Subsection 159 (2) of the Customs Act, the person may, upon summary conviction, be fined up to $50,000 and/or face up to six months in prison. Upon indictment, the person may be fined up to $500,000 and/or face up to five years in prison.'

Commenting on the possible implications of this provision, Danica Doucette-Preville, an associate in Gowling WLG's Calgary Office, told *WorldECR*, 'When there are concerns about restricted items being smuggled out of a country, it is good practice to impose vigilance on what is leaving through its borders. However, this new provision, if it passes through the legislative process and becomes law, will have consequences potentially not fully anticipated by the business community.'

The draft subsection, she also notes, must be read in conjunction with various other statutes, such as the Export and Import Permits Act, the Special Economic Measures Act, the United Nations Act, etc. One of these, the Export and Import Permits Act ('EIPA'), prohibits the export or transfer of any goods or technology included in a restricted items list, known as the Export Control List ('ECL'), without a permit issued by Global Affairs Canada ('GAC'), the Canadian government department responsible for administering the EIPA.

Traditionally, she explains, 'export' was understood as meaning the sending or provision of an item from Canada to a person outside Canada where the end-user and/or consignee was known. However, less well-known remains the fact that goods which are restricted under the ECL still require a permit even if they are only temporarily exported and 'the company retains control of the item the entire time it is outside of Canada, i.e. if a company employee brings restricted items to an international trade show.'

The Canada Border Services Agency and the Royal Canadian Mounted Police will enforce the new export smuggling provision in the Customs Act.

The new smuggling offence will not be in effect until Bill C-21 completes the legislative process. The date that the amendments to the Customs Act will come into effect will be established by Cabinet.

For further information, see:
http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8368535

Final rule on amendments to EAR and ITAR definitions

The Bureau of Industry and Security ('BIS') of the U.S. Commerce Department and the State Department's Directorate of Defence Trade Controls ('DDTC') have published final rules amending certain definitions as the agencies continue the process of aligning their respective regimes under the Export Control Reform ('ECR') initiative.

The changes relate to the definitions of 'access information', technology', 'required', 'foreign person', 'proscribed person', 'published', results of 'fundamental research', 'export', 'reexport', 'release', 'transfer', and 'transfer (in-country)', and are intended to enhance consistency between terms contained in the Commerce Department's Export Administration Regulations ('EAR') and the International Traffic in Arms Regulations ('ITAR'), governed by the U.S. Department of State.

The final rules also make revisions to the EAR and ITAR so as to update and clarify application of controls to electronically transmitted and stored technology and software, including by way of cloud computing.

The rules come into effect on 1 September 2016.

Further information is at:
http://www.bis.doc.gov/index.php/regulations/federal-register-notices#fr35586

U.S. to seek access to overseas visitors' social media profiles

A proposed regulation by the U.S. Department of Homeland Security ('DHS') would require travellers to the United States to share their social networking habits with the authorities in exchange for visa waiver entry.

The scheme, set out in a Federal Register notice by Customs and Border Protection ('CBP'), seeks access to details such as 'social media identifiers' – commonly referred to as usernames on social networking platforms such as Facebook and Instagram.

U.S. Customs and Border Protection ('CBP'), seeks access to 'social media identifiers' of those visiting the country.

Unliked

Even though revealing this information would be 'optional', as the proposal states, and the authorities would only be able to use it for 'vetting purposes, as well as applicant contact information,' some commentators have been critical of such a provision.

Joseph Lorenzo Hall, chief technologist at Washington, DC-based Center for Democracy and Technology, said, 'It's very hard to see travellers not filling out this item – even though it's optional – as they may fear not getting entry into the country.'

Edin Omanovic, a research officer at Privacy International, told *WorldECR* that he regards the proposal as 'an incredibly dangerous and knee-jerk response to real but complex security issues,' pointing out that despite its optional application, it could still be rolled out wider into more areas and place anyone choosing not to disclose such information under suspicion.

Omanovic said: 'People's social media profiles contain sensitive personal information – it is wholly inappropriate for state agencies to go through this information if there is no suspicion that a person has done anything wrong. Not only would this infringe on people's right to free speech, it would also lead to a huge amount of self-censorship, with individuals deleting anything from their social networks that they think U.S. authorities might not like.'

If implemented, the changes would affect Esta (Electronic System for Travel Authorisation) and Form I-94W applications. The proposal is open to public comment until 22 August 2016.

'No' to India's bid to join Nuclear Suppliers Group

In last month's issue of *WorldECR*, we reported that India had finally joined the Missile Technology Control Regime. A few weeks on, however, India's application for membership to the Nuclear Suppliers Group ('NSG') was blocked during the multilateral regime's 26th plenary meeting, held in Seoul on 23 and 24 June. The country's lack of membership to the Nuclear Non-Proliferation Treaty ('NPT') – described as the cornerstone of NSG membership – was cited as the key reason for opposition.

A public statement issued by the NSG stated that 'the NSG had discussions on the issue of "Technical, Legal and Political Aspects of the Participation of non-NPT States in the NSG" and decided to continue its discussion.'

China: 'not our fault'

The United States, which has publicly supported a New Delhi NSG bid, was outnumbered in the negotiations, with China reportedly blocking India's entry. However, China's state-run publication *Global Times* has rejected accusations in India that Beijing was solely responsible for turning down New Delhi's application to join the 48-member nuclear club. It said that at least nine other countries also opposed India's membership bid.

Hua Chunying, a spokesperson for China's foreign ministry, said that the NSG 'is still divided on the entry of non-NPT countries at the moment.'

'Regarding India's entry into the NSG, we have said many times that China holds a clear stance on the accession of non-NPT countries including India… China's position does not target any specific country, but applies to all non-NPT countries,' she added.

India formally applied to become a member of the NSG in May 2016. In light of India's commitments under the 2015 Paris Agreement of the 21st conference of the parties to the United Nations Framework Convention on Climate Change, the Ministry of External Affairs said its application had 'acquired an immediacy' and that 'an early positive decision by the NSG would have allowed [India] to move forward on the Paris Agreement.'

A public statement issued by the NSG is available at:

http://www.nuclearsuppliersgroup.org/images/2016_Public_Statement_Final.pdf

Congress to target Boeing-Iran deal

Measures passed by the U.S. House of Representatives could block the sale of U.S.-origin aircraft to Iran, potentially scuppering a $25bn deal between Boeing and Tehran.

Two amendments, authored by representative Peter Roskam, to an appropriations bill were approved earlier this month in Congress with bipartisan support. The amendments to the Financial Services and the General Government Appropriations Act are as follows:

- Amendment No. 45 prohibits the Office of Foreign Assets Control ('OFAC') from using funds to authorise a licence necessary to allow aircraft to be sold to Iran.

Proposed amendments threaten a $25bn deal for Boeing with Iran Air.

- Amendment No. 46 ensures Iran will not receive loans from U.S. financial institutions to purchase militarily-fungible aircraft by prohibiting OFAC from using funds to authorise the financing of such transactions.

Under these changes, a significant deal between Boeing and Iran Air – which would see the commercial airliner sell 109 777 and 737 aircrafts to the Iranian state-owned carrier for an estimated $25 billion – could be blocked.

Boeing's main competitor, Airbus, reached a similar deal with Iran regarding 118 jets worth $27 billion in January. There is speculation that that deal, negotiated by the European consortium with Iran, is likely to also be affected by OFAC regulations because of the quantity of U.S. content in the aircraft and parts.

Representative Roksam has been historically opposed to Western companies – particularly those in the military and defence sectors – doing business with Iran. In an op-ed published in *The Wall Street Journal* in April, Roksam urged Western companies not to invest in Iran; a month later he sent a letter to Boeing, urging the aviation company to not sell any commercial jet liners to Tehran as these could be turned into 'warplanes'.

'If you wouldn't do business with Islamic State, you shouldn't do business with the Islamic Republic,' he wrote.

New EU trade rules for torture goods

On 30 June, the European Permanent Representatives Committee ('COREPER'), acting on behalf of the European Council, approved an agreement with the European Parliament with regard to the sale and export of goods that can be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment.

The agreement amends a previous regulation governing such materials, in view of developments in this field since its introduction.

Under Regulation 1236/2005, the export and import of equipment that can only be used for torture or capital punishment had been banned since 2006, while specific licences were said to be obtainable for exports of goods that have similar uses, but which also have legitimate applications. In December 2011, the regulation was amended to include controls of the export of drugs that could be used in executions by lethal injection.

The agreement amends these controls to include:

- A ban on the brokering of equipment that is subject to a ban by any broker who is aware that goods may be used for torture or capital punishment;
- A ban on the supply of technical assistance concerning the listed goods by anyone who is aware that the equipment in question may be used for torture or capital punishment

The agreement also provides for a procedure in case a rapid amendment of the regulation's annexes is necessary when new goods enter the market.

The regulation is due to be approved by the Parliament in September, and will then be submitted to the Council for adoption.

Ukraine transit tit-for-tat 'counterproductive'

European Commissioner for Neighbourhood Policy and Enlargement Negotiations, Johannes Hahn has described Ukrainian responses to Russian-imposed restrictions on transit routes as 'counterproductive' and likely to deter the country's economic development.

The declaration comes shortly after Russian President Vladimir Putin issued a decree which further tightens the restrictions announced on 1 January 2016, which had put an end to the free-trade-area treaty between Russia and Ukraine, establishing that international transit road and rail transportation of goods from Ukraine to Kazakhstan through the territory of Russia must be carried out only from the territory of Belarus.

According to the recent amendments, these restrictions now also apply to transit to Kyrgyzstan, and introduce a full ban on transit of goods 'under embargo'.

In response to these new measures, Ukraine's Ministry of Economic Development and Trade announced a counter-package that mirrors some of the measures imposed by the Russian Federation.

Ukraine's Deputy Minister of Trade, Nataliya Mykolska said: 'We in the government believe that the additional restrictions introduced by the Russian Federation are a manifestation of commercial aggression against Ukraine. They are clearly contrary to the obligations of the Russian Federation in the framework of the World Trade Organisation and the agreement on the free trade zone.'

Commissioner Hahn noted that although he understood the Ukrainian government's plight, he believed that to immediately introduce countermeasures against Russia would be counterproductive in the long term. He also called on Russia to abandon the restrictions imposed on transit of Ukrainian goods.

Medical company fined for sanctions violations

The U.S. Treasury Department's Office of Foreign Assets Control ('OFAC') has fined a group of medical device and pharmaceuticals manufacturers more than $7.5million for violations of sanctions on Iran and Sudan.

OFAC says that Alcon Laboratories, Alcon Pharmaceuticals, and Alcon Management ('Alcon') violated the Iran sanctions on 452 occasions and the Sudan sanctions on 61 occasions when it engaged in the 'sale and exportation of medical end-use surgical and pharmaceutical products from the United States to distributors located in Iran and Sudan without OFAC authorization'.

Because it did not make a voluntary self-disclosure, the statutory maximum civil monetary penalty amount for the violations was $138,982,584, with a base penalty of $16,927,000. However, OFAC said that it had determined that the case was not egregious, as the violations had not significantly harmed U.S. sanctions objectives and the company had no prior sanctions history.

Alcon also reportedly took remedial action by ceasing the unlicensed exports to sanctioned countries, initiating an internal investigation of the violations, and instituting a robust compliance programme, which now includes updated or newly-created corporate export and trade sanctions compliance documents, enhanced trade compliance training, and enhanced compliance procedures for requesting licences.

In June, *WorldECR* reported that OFAC had fined medical goods company, HyperBranch Medical Technology Inc. $107,691.30 for apparent violations of sanctions on Iran.

BREXIT: now what happens?

The decision of a slim majority of UK voters to extract the country from the European Union throws up a myriad of questions, not least what will be the impact on the country's export controls and sanctions policies and regimes and what relationship will the UK establish with the rest of Europe. *WorldECR* asked practitioners both in the UK and out what their fears and expectations might be.

The UK referendum, in which voters decided by a slim margin that the country should leave the European Union, strip themselves of their rights as EU citizens and leave the Common Market, has sent financial and political shockwaves well beyond the 28 EU Member States.

The widely unexpected decision fundamentally alters Britain's relationship with its non-EU trading partners, casts a shadow over its desirability as an investment target and its role generally in the international community.

Indeed, many tears and much ink have been shed (and many heads disbelievingly nodded) since Thursday 23 June – but newly crowned Prime Minister Theresa May (who supported the 'Remain' side in the run-up to the referendum) has insisted that 'there's no going back'. The questions remain when, how, and with what repercussions. As former UK diplomat Richard Tauwhare (now with the law firm Dechert) points out: 'Before we actually reach the stage of negotiating our exit, the government will want to consult widely with industry and with the other governments. But the question is, what can we actually achieve? Some appear to expect that we can have our cake and eat it too [i.e. able to enjoy some of the benefits of a free market, such as tariff-free trade, whilst introducing restrictions on free movement], but that really depends on what can be negotiated.'

This uncertainty pertains as much to the world of trade compliance as it does to all the other Pandora's Boxes flung open by the national bid to reclaim 'sovereignty'. But the consensus appears to be that change will be awkward, but not necessarily abrupt:

As Pierre Cardin, Airbus Group Export Compliance Officer, pointed out to *WorldECR*: 'The UK itself is a member of all the relevant international export control agreements (the Wassenaar Arrangement, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Australia Group). These memberships are not contingent on the UK's EU membership and, therefore, until the Brexit is fully implemented we must not expect major changes in the manner in which the UK issues export licences for either defence or dual-use goods.'

'[U]ntil the Brexit is fully implemented we must not expect major changes in the manner in which the UK issues export licences for either defence or dual-use goods.'

Cardin points out that all the ensuing questions – for example, whether there will be a resulting weakening in the project to more closely harmonise export control rules, or an impact on sanctions regimes – will augur 'the beginning of what will be a new responsibility of compliance officers: predicting the outcome of the Brexit negotiations between the EU and the UK and anticipating the consequences for daily operations…'

Allison Porcella, Head of Trade Compliance at Zurich's STR Technologies, is similarly unfazed. She says that at least from her perspective the anticipated departure 'will have the most impact on customs procedures, rather than licensing or sanctions policy.'

'I don't foresee there being burdensome changes in the compliance landscape,' she says, 'as the UK is already a sophisticated trading country/economy. Rather, I see the impact being operational and financial – where a compliance officer can support in identifying the "what-if's" and contribute to the future strategic planning around the possibilities.'

Twenty questions

In essence, there are both

Focus: BREXIT

micro and macro elements to the uncertainties: That the UK's Export Control Organisation ('ECO') – currently the 'competent authority' under EU Dual-Use Regulation – will manage the transition necessary for the licensing is not in doubt. But Britain's withdrawal from the EU's Council of Europe raises profound questions about the future roles of both.

As regards the exports of dual-use goods between the UK and the EU, Jaco Wessels, export control officer at Dutch manufacturer AkzoNobel (which has production facilities in the United Kingdom), says he expects that the ECO will issue 'a general licence for the other 27 countries, and recognition and reciprocity for that within the European Union.'

From her vantage point in Washington DC, IBM's Lillian Norwood (manager in the company's export regulation office) says that her greatest concern is about how the existing export policies and authorisations may change once the departure is completed. In particular, she points out, 'the EU's ability to freely move goods amongst participating members will no longer be available for the UK. Will there be UK general authorisations issued which will allow these types of activities to continue or will individual export licences need to be obtained? I'm not as concerned with U.S./UK relations and impacts to how UK is treated from a control point of view as UK remains a strategic partner to the U.S.'

Dechert's Richard Tauwhare would think that Norwood should be reassured about the probability of the status-quo being essentially maintained: 'The bottom line is that the UK is still a full member of all the international export control regimes. The baseline control lists are the same, and Brexit won't change our discretion to add others. The ideal would be that we arrive at a licence-free agreement with the EU. Failing that, they could extend EU001 [EU General Export Authorisation] to the UK and this could be mirrored in a new UK OGEL [open general export licence] covering the EU.'

Former chess champion-turned-political commentator Gary Kasparov recently described the UK's departure from the EU as 'the perfect gift' for the Russian president.'

With regard to exports beyond the European Union, he suggests, 'We'd likely continue much as we are. We could mirror the EU's general export authorisations and there wouldn't be much overall change. The bigger change could be in customs procedures. If we leave the EU Customs Union and sign free-trade agreements with India and China, for example, that would have major repercussions.'

Brussels-based trade lawyer John Grayston suggests that if the UK's intention is to cut a new deal with Europe (along the lines of those agreed between Brussels and non-EU members of the European Economic Area, Norway and Switzerland), '...then even if this is possible it will likely take a long time.'

On the other hand, if the UK insists on cutting its ties – for example, by withdrawing from the 'free movement' provision that currently underpins the Common Market, then a deal could be reached more quickly. 'In theory,' says Grayston, 'this could provide business with the certainty needed to restore confidence. But this will also depend on how quickly the UK can put in place "beneficial" trade measures to replace those currently provided by the EU.'

Grayston notes that 'The biggest impact of Brexit for export control will in practice be felt by those trading in dual-use items because movements from EU to UK and vice-versa will become exports'.

In line with Tauwhare's suggestion, he says that the EU may need to add the UK to the list of approved third countries for the purposes of UGEA 001. The UK will need to replace the EU Dual-Use Regulation with a similar measure in order to be able to adopt a 'UK001' general licence to cover specified exports to the EU (and other third countries covered by UGEA001). The unavoidable consequence will in, his view, be 'an additional compliance burden for trade between the EU and UK because while general licences may remove the need for individual licensing, they nevertheless impose record-keeping obligations which do not exist for trade between EU Member States.'

What of sanctions?

But it is the sanctions dimension that raises the big questions: Vladimir Putin is believed to be one of the few non-EU/UK fans of 'Brexit' – former chess champion-turned-political commentator Gary Kasparov recently described the UK's departure from the EU as 'the perfect gift' for the Russian president – weakening its borders and fostering division within. So, for how long will the UK and EU sing the same tune *vis-a-vis* 'The Great Bear'? And for how long will Britain be able to bear being outside of the European Council – and thus decision-making on matters pertaining to the Common Foreign Security Policy ('CFSP')?

'In all likelihood,' says Tauwhare, 'the UK government will want to still be included in the dialogue, although of course we won't be in the Council of Ministers. If we remain in the European Economic Area we could have some input. But will we want something more?'

Tauwhare doesn't hold with the idea that Brexit of itself will weaken the CFSP: 'The remaining 27 have signalled their intention to intensify their cooperation. The UK not being there will free them to go further faster. As regards sanctions, remember that mostly they flow from the Security Council, of which the UK remains a permanent member. But there is room for concern that without the UK any additional measures taken by the EU, for example against Russia, may not be as robust as we would like. The UK will retain its existing option to introduce tougher sanctions on a national basis. But of course every time that we're out of step, it risks

disadvantaging UK business since EU companies could provide goods or services that UK companies were prohibited from supplying.'

Maya Lester QC, a London-based barrister who frequently appears in sanctions cases before the European Court of Justice, points out that splitting the UK judiciary away from the EU may have any number of effects: 'It means that if the UK were to take additional sanctions measures that would mean that more cases would be subject to judicial review in the UK courts. There could also be scenarios where the EU and the UK both sanction the same individuals or entities on account of the UN listings. That raises *Kadi*-type issues – to what extent do the EU and others have any discretion to do anything other than follow the United Nations in designating entities or individuals? And how will it play out if the UK and EU courts, faced with parallel challenges, reach divergent conclusions?'

Lester adds that there are human considerations too: UK lawyers have contributed greatly to the development of the EU judiciary where they've played key roles.

New statesmen

As at time of writing, Britain's new Prime Minister Theresa May has appointed much of her new cabinet, including, as Foreign Secretary, Boris Johnson – the man who led the campaign for Britain to leave the European Union.

The appointment surprised many. In April, Johnson imputed 'part-Kenyan' President [Barack Obama's] support for the UK remaining in the EU to his 'ancestral dislike of the British empire'. Of presidential candidate Hillary Clinton, he's previously written (in an article endorsing her presidential prospects): 'She's got dyed blonde hair and pouty lips, and a steely blue stare, like a sadistic nurse in a mental hospital.' Evidently, as the UK leaves Europe, we're also set to establish a new course of statesmanship.

Questions compliance professionals are asking

Exporting from the EU

- Will I be able to use the EU common general export authorisations ('CGEAs') for exports to the UK?
- Will the UK get a status similar to that of Switzerland?
- Will Scotland enjoy special privileges if they go for independence from UK?
- Will I get export licences if my supplies are for certain military end uses (Trident programme = WMD) etc.
- Will existing licences remain valid, or will they have to be returned/re-applied?

Exporting from the UK

- What type of licences will BIS introduce for my licensable exports to EU countries?
- How do I have to treat Scotland if they strive for independence?
- Will the UK implement its own sanctions regimes?

U.S. (re-)exports

- Will the UK remain eligible for the many privileges it now has?
- What will the changes – if any – mean for me as a re-exporter?

Thank you to Ralph Wirtz, Head of Group Trade Control, Oerlikon

CYPRUS

New law to enforce international sanctions

By Costas Stamatiou, Neocleous

www.neocleous.com

The Department of Merchant Shipping has issued a circular to owners, operators and managers of Cyprus ships informing them of the recent enactment of the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the European Union Council Decisions and Regulations (Restrictive Measures) Law of 2016.[1]

The law obliges every person or entity in Cyprus to abide by and comply with all sanctions or restrictive measures imposed by UN Security Council or EU resolutions. Article 3 of the law makes individual ministries responsible for:

- ensuring the observance of sanctions that fall within the scope of their operations;
- issuing any appropriate instructions to the persons and entities under their supervision;
- and taking enforcement action in the event of non-compliance.[2]

The law imposes penalties in cases of non-compliance (up to two years' imprisonment, a fine of €100,000 or both for individuals and a fine of €300,000 for legal entities). Further, the competent authority is required to report the violation of any sanctions to the police for investigation and the customs authorities may compound offences under the law with offences under the Customs Code Laws.

Links and notes

[1] Law 58(I)/2016, published in the Official Gazette 4564, Supplement I(I), April 25 2016.

[2] Under the provisions of Article 59(6) of the Prevention and Suppression of Money Laundering from Unlawful Activities Laws.

RUSSIA

Russia extends embargo on EU, U.S. and other food and agricultural products

By Yana Dianova, Grata Law Firm

www.gratanet.com

By the Decree of the President of the Russian Federation ('the RF President') No. 305 dated 29 June 2016 the period of effectiveness of the special economic measures – the embargo on import of certain agricultural products, foods and raw materials originating from countries that imposed economic sanctions on Russia – was extended from 6 August 2016 through 31 December 2017. The government of the Russian Federation ('the RF Government') is instructed to take the necessary measures for the implementation of the Decree No. 305, as well as to submit proposals for change of the period of effectiveness of the respective special economic measures. The embargo was first established by the Decree of the RF President No. 560 dated 6 August 2014 and then extended by the Decree No. 320 dated 24 June 2015. The Decision of the RF Government No. 1458 No. 560 dated 7 August 2014 (as amended) specifies:

1. the countries of origin of agricultural products, raw materials and foods: Albania, Australia, Canada, Iceland, Lichtenstein, Montenegro, the EU member-states, the Kingdom of Norway, the Ukraine[1] and the United States of America;
2. the list of agricultural products, raw materials and foods banned for import in Russia (referring to the Foreign Economic Activity Commodity Classification of the Customs Union) originating from the mentioned countries which are banned for import in Russia (the 'banned products'), that includes:
   - meat of cattle and pork (fresh, chilled and frozen (with some exceptions));
   - meat and edible by-products of certain poultry (fresh, chilled and frozen (with some exceptions));
   - salty, dried, smoked meat and meat in brine;

- fish, shell fish, mussels and other aquatic invertebrates (with some exceptions);
- milk and milk products, including prepared products like cheese and cottage cheese (with some exceptions);
- vegetables, edible roots and tube crops (with some exceptions);
- fruit and nuts;
- sausages and other products from meat, meat by-products or blood; food products prepared on their basis;
- milk-containing food products and products on the basis of vegetable oils;
- food or finished products manufactured with the use of cheese production technologies and containing 1.5 and more weight percent of milk fat.

The Federal Customs Service of the Russian Federation ('the FCS of Russia') controls the compliance with the embargo on import in Russia of the respective products. According to the Order of the FCS of Russia No. 1496 dated 7 August 2014, the heads of regional customs offices and customs directly reporting to the FCS of Russia, in particular, take the following measures:

a. ensure the determination of the country of origin of the products imported to the customs territory of the Customs Union[2] according to the established procedure, including actual control within the risk management system, if required;
b. in case the facts of declaring of the banned products are detected, refuse [to] release of such products according to the declared customs procedure and take measures for their immediate export from the customs territory of the Customs Union.

Furthermore, the banned products imported to Russia are subject to destruction according to the Decree of the RF President No. 391 dated 29 July 2015. The products imported by individuals for personal consumption or placed under the customs procedure of customs transit and being transported to third countries are exempt from the Decree No. 391 subject to compliance with the following conditions:

- veterinary and phytosanitary accompanying documents for such products are authentic and comply with the products;
- the state controlling authorities have the grounds to consider that the products will actually be delivered to a place outside the territory of Russia, in accordance with the conditions for the customs procedure of customs transit.

The Regulations on destruction of agricultural products, raw materials and food products included in the list of products originating from Albania, Australia, Canada, Island, Lichtenstein, Montenegro, the EU member-states, the Kingdom of Norway, the Ukraine and the United States of America that are prohibited for import in the territory of the Russian Federation are approved by the Decision of the RF Government No. 774 dated 31 July 2015.

According to the Regulations a decision on confiscation and destruction of the banned products is taken by authorized officers of the FCS of Russia or the Federal Service for Veterinary and Phytosanitary Supervision or the Federal Service for Supervision in the Domain of Consumer Rights and Human Welfare upon detection of the fact of performing of foreign economic operations contemplating import in Russia of the banned products, irrespective of whether or not the person (persons) performing such operations has been detected.

Links and notes

[1] With respect to the Ukraine the embargo applies from 1 January, 2016.

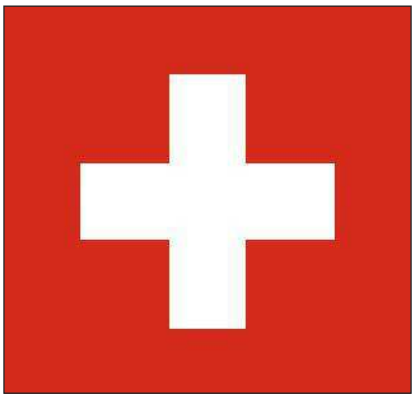
[2]. According to Article 2 of the Customs Code of the Customs Union the common customs territory of the Customs Union comprises the territories of the Republic of Armenia, the Republic of Belarus, the Republic of Kazakhstan, Kyrgyz Republic and the Russian Federation (the member states of the Customs Union), as well as artificial islands, installations, fixtures and other facilities located outside the territory of the member states of the Customs Union with respect to which the latter have jurisdiction.

SWITZERLAND

Switzerland tightens sanctions against North Korea

By Andreas Glarner, Peter Henschel, MME Compliance

www.mme.ch



The Federal Council of Switzerland decided to impose considerably tighter sanctions on the Democratic People's Republic of Korea ('DPRK'), thereby implementing Resolution 2270 (2016) of the UN Security Council. The new provisions entered into force on 18 May.

In response to the nuclear and missile testing carried out by North Korea on 6 January and 7 February, the UN Security Council issued Resolution 2270 (2016) on 2 March 2016, thus significantly tightening existing sanctions against North Korea. The resolution covers more extensive restrictions on the trade in goods, financial transactions, maritime and air transport and in the education sector. As a result of the numerous amendments required, the current ordinance will now be completely revised.

The existing ban on exports for

luxury goods has been expanded to include additional products (luxury watches, certain recreational vehicles such as personal watercraft and snowmobiles, items of lead crystal and recreational sports equipment etc). To ensure that no prohibited products are being exported to DPRK, exports and the transit of consignments of goods will now be checked by customs. The export and transit of goods bound for DPRK must be authorised by the State Secretariat for Economic Affairs ('SECO') in advance.

In a new move, the export of goods that could possibly increase the operational capabilities of the North Korean army has been prohibited. Furthermore, the sale and supply of certain aviation fuels is also prohibited. Also prohibited is the purchase of certain raw materials (coal, iron, gold and certain types of ore and rare materials) from DPRK.

The financial sanctions (the freezing of assets and a ban on the provision of finances) now apply to a wider group of individuals. All funds and economic resources connected with North Korea's nuclear and missile programmes have been blocked. This also applies to funds and economic resources owned or controlled by the Korean Regime. Swiss banks are prohibited from opening branches, subsidiaries or agencies in North Korea, while existing branches and bank accounts in North Korea must be closed by 2 June. Conversely, North Korean banks are prohibited to run subsidiaries or branches in Switzerland.

In the education sector, citizens of the DPRK will not be permitted to take certain courses (such as higher physics, advanced computer simulation or nuclear engineering). Moreover, military, paramilitary and police training for instructors, consultants and government officials from North Korea is also prohibited.

U.S.A.

BIS issues final rule revising enforcement guidelines

By Meghan Hamilton, Maria H. van Wagenberg and Janet K. Kim, Baker & McKenzie

www.bakermckenzie.com

On 22 June 2016, the U.S. Commerce Department's Bureau of Industry and Security ('BIS') published a final rule ('Final Rule') revising its guidance regarding penalties in administrative enforcement cases under the Export Administration Regulations ('EAR').

The Final Rule will go into effect 30 days after its publication or on 22 July 2016. Specifically, the Final Rule amends the Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases ('BIS Guidelines'), found in Supplement No. 1 of Part 766 of the EAR, to make BIS's civil penalty determinations more predictable, transparent, and consistent with the Economic Sanctions Enforcement Guidelines implemented by the Treasury Department's Office of Foreign Assets Control ('OFAC'), Appendix A to 31 C.F.R. Part 501 ('OFAC Guidelines').

In the Final Rule, BIS emphasised that it does not believe the new BIS Guidelines will meaningfully affect the percentage of voluntary self-disclosures that result in civil monetary penalties, which is currently at about 3%. It is not clear whether the new BIS Guidelines will result in higher civil monetary penalties in cases where they are imposed, particularly those involving violations that were not voluntarily self-disclosed, or in other significant changes to the enforcement practices of the Office of Export Enforcement ('OEE') (the organisational unit of BIS responsible for enforcement). Nonetheless, the BIS Guidelines may have the following implications for companies subject to enforcement actions under the EAR:

Alignment with OFAC Guidelines

The new BIS Guidelines will make OEE's penalty determinations more aligned with those of OFAC, particularly with respect to sanctions enforcement cases where both BIS and OFAC may exercise jurisdiction. Since expiration of the Export Administration Act of 1979 (P.L. 76-72) ('EAA') in 1994, BIS has operated pursuant to the authority of the International Emergency Economic Powers Act ('IEEPA'), which is the same statutory authority underlying most of OFAC's sanctions programmes. Maximum penalties under IEEPA are the same for both EAR and OFAC violations: 20 years' imprisonment and/or $1 million per violation for criminal penalties and $250,000 (as adjusted for inflation) or twice the transaction value (whichever is greater) for administrative monetary penalties.

Expanded range of enforcement responses

Whereas the prior guidelines provided only three possible responses to violations (i.e., a warning letter, an enforcement action, or a criminal referral) and three types of administrative sanctions (i.e., civil monetary penalties, denial orders, or exclusion from practice), the BIS Guidelines now set forth a range of possible responses that include all of these actions and the following additional enforcement options:

- Issuance of a 'No Action' letter in cases where OEE has insufficient information to determine whether a violation occurred, determines a violation did not occur, or believes

the conduct does not warrant an administrative response;
- Suspension, revision, or revocation of licences or the availability of licence exceptions;
- Requirements for training, audits, or other compliance measures; and
- Suspension or deferral of civil monetary penalties during a probationary period, in which the company may be required to allocate an equivalent amount to required training, audit or compliance activities. While OEE has allowed for suspension or deferral of civil monetary penalties, this was previously done primarily on the basis of financial need.

Enhanced predictability of monetary civil penalties

For cases where a monetary civil penalty is deemed appropriate, the BIS Guidelines set out a two-part calculation by which the penalty amount would be determined:

(1) First, a base penalty amount would be determined, based on (a) whether the matter is deemed to be 'egregious' or 'non-egregious' and (b) whether the matter is disclosed through a voluntary self-disclosure (in which case, at least a 50% penalty reduction will apply) or through some other source. The base penalty calculations can be summarised as follows (subject to adjustment for inflation, as noted above):

- In a non-egregious, voluntarily self-disclosed case, the base penalty amount will be one-half of the transaction value (capped at $125,000 per violation);
- In a non-egregious, non-voluntarily self-disclosed case, the base penalty amount will be the 'applicable schedule amount,' as defined in the BIS Guidelines (capped at $250,000 per violation);
- In an egregious, voluntarily self-disclosed case, the base penalty amount will be up to one-half the statutory maximum (the greater of $125,000 or the transaction value); and
- In an egregious, non-voluntarily self-disclosed case, the base penalty amount will be up to the statutory maximum (the greater of $250,000 or twice the transaction value).

These base penalty amounts match those set out in the OFAC Guidelines, except that, in egregious cases, BIS has the discretion to adjust the base penalty downward from the statutory maximum or one-half the statutory maximum, whereas comparable language in the OFAC Guidelines does not provide this flexibility to OFAC.

(2) Next, BIS would then adjust the base penalty amount downward or upward (up to the statutory maximum) on a case-by-case basis, based on the presence of aggravating, general, and mitigating factors. The new BIS Guidelines now provide examples of conduct under each factor and some specific penalty reduction percentages in an attempt to provide clarity for how each factor is applied to a given case. For example, a first offence will generally result in a 25% reduction, while exceptional cooperation will generally result in a 25-40% reduction; maximum mitigation for any case other than a non-egregious, voluntarily self-disclosed case will generally not exceed 75% of the base penalty.

Continuing importance of voluntary self-disclosures

The Final Rule makes clear that the BIS Guidelines are intended to emphasise and incentivise voluntary self-disclosures. According to the Final Rule, the BIS Guidelines formalise OEE's longstanding practice of giving up to 50% in penalty reductions for such disclosures.

Increased pressure to settle before charges are filed

The BIS Guidelines also provide that penalties will likely be higher in cases that settle after the commencement of litigation. In practice, this means companies may be under greater pressure to settle before litigation.

The new BIS Guidelines will not apply to pending enforcement matters where, as of 22 July 2016, settlement negotiations are ongoing and no charging letters have been filed. In addition, the new BIS Guidelines will not apply to violations of Commerce's anti-boycott rules, 15 C.F.R. Part 760, which will continue to be subject to the enforcement guidelines in Supplement No. 2 of Part 766 of the EAR.

GOING NUCLEAR

WorldECR speaks to the NEI's Ted Jones.

Ted Jones joined the U.S. Nuclear Energy Institute ('NEI') in 2010 as director for supplier international relations. He'd previously served as a director with the U.S.-India Business Council at the U.S. Chamber of Commerce, where he played a critical role in advocating for approvals from the U.S. Congress to admit India into global nuclear trade.

At the time that Ted Jones joined the U.S.-India Business Council in 2005, he says, 'India was new to me and so was the nuclear industry.' But that changed when the United States and India agreed a new strategic partnership that promised to bring India into the global mainstream of nuclear nonproliferation and civil nuclear commerce.

At the core of the U.S.-India Civil Nuclear Agreement was India's assent to separate its military and civilian nuclear facilities and place the civilian facilities under International Atomic Energy Agency ('IAEA') safeguards – in return for which, the United States would work towards India's resumption of nuclear trade with the world. The deal represented a controversial change in U.S. policy, which had effectively isolated India from global nuclear commerce since it exploded a nuclear device in 1974. In September 2008, the Nuclear Suppliers Group – the cartel of nuclear supplier countries created to deny peaceful nuclear energy to India and other states outside the global nonproliferation regime – effectively ended India's isolation by approving a waiver for the country.

By the time the U.S.-India deal was sealed in 2008 with the final approval of the U.S. Congress for a bilateral nuclear cooperation agreement, Jones' move to NEI (in essence, the successor of the Atomic Industrial Forum, created in 1953) was a natural step.

Higher hurdles for U.S. nuclear suppliers

As the policy organisation for the nuclear energy industry, NEI quite naturally believes that the United States should be promoting its nuclear export industry, and the U.S. government has long viewed nuclear energy supply arrangements as a powerful tool for maximising U.S. influence on global nuclear safety, security and nonproliferation.

The U.S. Department of Commerce estimates that the international market for equipment and services will be worth between $500 billion and $740 billion over the next 10 years, and that 'every $1 billion of exports by U.S. companies supports 5,000 to 10,000 domestic jobs.'

It points out that right now, there are 63 new power stations under construction with a further 160 'in the licensing and advanced planning stages' – and that 'demand for high-quality commodities, components and services provides an export opportunity for U.S. manufacturers.'

'For a long time, the U.S. nuclear export control regime has been more complex, more restrictive and less efficient than the regimes of other leading nuclear supplier countries. '

In the view of U.S. industry, inefficient export licensing creates an uphill struggle for U.S. companies to actually take advantage of those opportunities.

Jones points out that the U.S. industry must contend with a complex, three-part export controls system that is administered by three different agencies:

- The U.S. Nuclear Regulatory Commission ('NRC') administers controls over exports of nuclear reactors, components and materials, as well as fuel cycle facilities, codified at 10 CFR Part 110;
- The U.S. Department of Energy ('DOE') administers controls over exports of nuclear technology and technical assistance, in accordance with its regulations governing 'assistance to foreign atomic energy activities' (10 CFR Part 810). Within the DOE, the National Nuclear Security Administration ('NNSA') administers Part 810;
- The U.S. Department of Commerce's Bureau of Industry and Security ('BIS') administers controls over exports of commercial and dual-use commodities and technology, including commodities and technology for the balance of plant, in accordance with the Export Administration Regulations ('EAR'), codified at 15 CFR Parts 730-774.

Jones explains: 'The Department of Commerce handles dual-use technologies. The Nuclear Regulatory Commission administers Part 110, which governs the actual items.'

According to Jones, 'For a long time, the U.S. nuclear export control regime has been more complex, more restrictive and less efficient than the regimes of other leading nuclear supplier countries. In a highly

competitive global market, this imposes a significant competitive disadvantage on U.S. suppliers.'

From the perspective of industry competitiveness, Jones says that the Part 810 regulation governing nuclear technology exports remains the most problematic. 'Part 810 is so critical because it regulates commercial activity early in the tender process,' Jones explains. 'And it has been applied broadly to all sorts of proprietary information relating to the nuclear plant, requiring a supplier to obtain a Part 810 authorisation in order to have a meaningful commercial discussion with an overseas customer. Our competitors are able to get their equivalent [authorisation] within something between five weeks and four months. But for a Part 810 authorisation, one year is more typical. We know of many cases in which U.S. suppliers were forced to pull out of tenders because they could not obtain a timely authorisation.'

The Department of Energy did indeed last year publish amendments to the Part 810 Regulations – these constituted the first significant revision of the regulation in almost three decades.

In 2012, NEI commissioned law firm Pillsbury Winthrop Shaw Pittman to undertake a comparison of the U.S. nuclear export control regimes with that of five other members of the Nuclear Suppliers' Group ('NSG'): Russia, France, Korea ('ROK') and Japan.

Generally, the Pillsbury study concurred with the NEI's longstanding complaint that, for multiple reasons, U.S. nuclear exporters bear a competitive disadvantage, primarily due to inefficiencies in the Part 810 authorisation process.

The report also pointed out that 'DOE's Part 810 controls on exports of technical data and technical assistance are more broadly worded than the NSG's controls on information for the "development," "production" and "use" of controlled commodities. Thus, DOE has authority, under 10 CFR Part 810, to control a broader range of activities by U.S. persons than is provided by national laws that control technology exports based on the NSG Guidelines.'

With few new nuclear plants likely to be built in the United States in the near term, U.S. suppliers need to access the growing international markets in order to remain viable.

Pinning hopes on process reforms

But Jones says that the regulatory requirements of Part 810 are not in themselves the most significant problem for U.S. nuclear exporters. The greater problem lies in the inefficiencies of the authorisation process.

'For industry,' he says, 'the bottom line is getting an export licence in a predictable and timely manner. The study's top-line conclusion that Part 810 is significantly less efficient – typically requiring more than a year – remains as valid today as ever.'

In 2013, the U.S. Department of Energy acknowledged the commercial risks of inefficiencies in the Part 810 authorisation process and announced a Process Improvement Program to remedy the problem.

One of the Energy Department's efficiency reforms, completed this year, is published guidance for compliance with the rule. The guidance clarifies for the first time key terms such as 'foreign national', 'production' and 'technology,' and articulates issues such as when 'operational safety' information and assistance can be provided under a general authorisation regardless of destination country.

Two factors contributing significantly to delays lie in the 'spaghetti bowl' that is the U.S. government inter-agency review, and the length of time that it takes to obtain the necessary nonproliferation assurances from the foreign government. On both counts, Jones believes, there's hope.

On the former, he says the government has taken on Six Sigma experts to look at the processes involved with the aim of streamlining them and cutting out unnecessary administrative time.

And on the latter, he notes: 'For certain countries, delays from government assurances are worse than for others. And the U.S. government is trying new approaches. For example, China and the United States have agreed to implement a process to enhance nonproliferation assurances while expediting Chinese government for certain approved Chinese entities.

Going forward safely

Worldwide, the nuclear energy industry appears to have bounced back since the March 2011 accident at Fukushima. And the U.S. nuclear energy industry has high expectations for the large and growing nuclear energy global market. In terms of meeting global demand, Russia presents a 'formidable rival', says Jones, not least because the level of government backing of the industry, which sees (state-owned) nuclear suppliers cutting deals that private sector companies would blanch at:

'The U.S. nuclear energy industry will never be a national one like Russia's. But there are things that our government and industry can do together to make our companies competitive – and that's one of our areas of focus.'

In time, Jones says, China will also play a major role in the energy market as a supplier. For now, the greater focus is meeting the domestic need. With 22 plants under construction and many more planned, China will be generating more nuclear energy than the United States by 2032.

For the moment, then, 'China represents a huge market for U.S. nuclear exports,' Jones says. By one estimate, China is set to spend $1 trillion between now and 2050 as it pushes to wean itself from fossil fuel-based energy generation – potentially creating thousands of jobs in the global nuclear supply chain.

Westinghouse is seeking to conclude agreements for plants beyond the four AP1000s currently under construction; last September, Terrapower, another U.S. company, signed off on a joint venture with the China National Nuclear Corporation to build a next-generation sodium-cooled fast reactor that uses depleted uranium as fuel.

But while China often steals the headlines, by no means is it the only growth market. India is also actively seeking to increase the proportion of power that it generates through nuclear generation, while countries in regions such as the Middle East, Eastern Europe – notably the Czech Republic and Poland, and SE Asia – either already have nuclear power programmes in place or are actively developing them.

'A strong part to play'

U.S. national interest in nuclear exports goes beyond the economic benefits of projects abroad: 'It's also about maintaining a domestic industrial base and U.S. technology leadership for U.S. energy security and national security,' says Jones.

With few new nuclear plants likely to be built in the United States in the near term, U.S. suppliers need to access the growing international markets in order to remain viable. If they are unable to compete in those markets, they would be in a weak position to continue supplying the U.S. domestic fleet of plants. And because elements of the U.S. nuclear energy also supply the U.S. military, there is a national security aspect as well.

Across the world, says Jones, 'U.S. nuclear suppliers have a strong role to play. We exert a beneficial influence over nuclear nonproliferation policy and practices, and help to ensure the highest possible levels of nuclear power plant safety and reliability with advanced reactor designs and world-class operational expertise. For countries that are developing nuclear energy for the first time, the U.S. nuclear industry is a proven partner for industrial development. In order to achieve these benefits, the U.S. commercial nuclear energy sector must participate in the rapidly expanding global market for nuclear energy technologies. And I do believe that our regulatory authorities recognise this.'

Now for something totally different

Clearly, the foreboding-laden editorial carried in our previous issue failed to stave off the prospect of the United Kingdom leaving the European Union (does the Press no longer count for anything?!). Anyone in the country at the time that the referendum result became strikingly clear will vouch for the fact that the mood amongst those that voted to Remain was disbelieving and sombre, and, for the most part, muted amongst those whose will prevailed.

The compliance community – a glass-half-full sort of a bunch – appears to remain for the most part phlegmatic about the result. In day-to-day terms, life will probably became a little more onerous, but for the most part largely unchanged: general licences and mirroring legislation can serve to plaster and poultice the bureaucratic sprains wrought upon business by Brexit (so much for the EU being the mother of all red tape).

But the bigger, existential questions remain. Take, for example, the extraordinary drama taking place in Turkey. Will the United Kingdom tow the same line with Ankara as Brussels does? While the UK remains a part of the EU for the moment, does it still have a role to play in the EU's Common Foreign and Security Policy? And as the UK withdraws from Europe, will Washington lose a trusted ambassador in Brussels?

An acquaintance who visited the Foreign and Commonwealth Office days after the referendum told me that the FCO 'has absolutely no idea what the next steps are, because nobody ever thought it would happen'. For the moment, the world can take comfort in the mirth occasioned by the fact that the Foreign Secretary has in his previous life lampooned or insulted many of the world leaders – and their subjects – whom he will now be obliged to consider colleagues and allies.

While the UK remains a part of the EU for the moment, does it still have a role to play in the EU's Common Foreign and Security Policy?

Shortly after the BREXIT shock, but a whole seven years after its having been commissioned, the two-million-word thundering tome that is Lord Chilcot's inquiry into the Iraq War landed with a solemn thump on the national conscience. It told the world nothing that it hadn't figured out for itself years ago (the Iraq War was based on faulty intelligence which, wilfully or otherwise, no-one had been inclined to check, that the result had been disastrous and that, 'Despite explicit warnings, the consequences of the invasion were underestimated. The planning and preparations for Iraq after Saddam Hussein were wholly inadequate.' Is there a lesson buried cryptically away in all this that clever politicians might disinter and decipher?

It strikes me that so much of the compliance function involves responding to the actions of government. Law and policy are typically imputed to be attributable to fine motives such as national and international security – but politicians are neither infallible nor are they immune to the diversionary temptations of vanity, venality, self-importance and their own short-term interest.

The world moves quickly and surprisingly, anticipating, say, technological development is no guarantee of pre-empting threats (as the horrific events in Nice demonstrated earlier this month).

Does this mean then, that business needs to make its own assessments and contingency planning, and not rely wholly on the dicta of government, if it is to meet its 'compliance' obligations in the fullest sense of the term?

Tom Blass, July 2016
TNB@worldecr.com

Iran: Still a sanctions minefield for non-U.S. companies


Iran may appear to be opening up for investment from outside, but there are a host of U.S. sanctions-related hurdles in the way, particularly for non-U.S. subsidiaries of U.S. companies. Ed Krauland and Peter Jeydel look at the risk points non-U.S. Persons will need to address before going into Iran.

Those who got swept up in the expectation that the Iran nuclear deal would allow non-U.S. companies, particularly subsidiaries of U.S. companies, to re-enter the Iran market worry-free have probably already begun to realise that was not on the cards. While non-sanctions related obstacles – such as those directly associated with money laundering control vulnerabilities in the financial system, perceptions of corruption, the state of regulatory or commercial frameworks, and possible uncertainty concerning Iran's domestic and regional political future – present significant risks to business, as does the 'de-risking' approach banks and other financial service providers have adopted (understandably), there are also significant legal complexities and risks that remain in place, even for non-U.S. companies. The true picture is sobering once it comes into focus.

Following the Joint Comprehensive Plan of Action ('JCPOA'), the U.S. government did lift or suspend most, though not all, of the sanctions aimed specifically at non-U.S. persons and entities (so-called 'secondary sanctions'). It has also authorised a wide spectrum of activities that were previously prohibited for non-U.S. subsidiaries of U.S. companies under the Iranian Transactions and Sanctions Regulations ('ITSR'). However, many of the core U.S. sanctions risks have not materially changed, certainly not for U.S. companies, and significant risks remain for non-U.S. companies as well, given the potentially long supply and sales chains that reach back into the United States. Furthermore, the relief that has been offered under the ITSR for non-U.S. subsidiaries of U.S. companies is more complicated than many may have expected. Added to this is the fact that the U.S. government, as well as other national, EU or UN authorities, can impose new sanctions on Iran – for example, relating to ballistic missiles, human rights, terrorism or WMDs. And the risk of 'snapback' of the nuclear-related sanctions, should the JCPOA fail, would lead to a return of the status quo ante.

This article provides an overview of the U.S. sanctions measures that will continue to complicate any sanctioned country business that has a U.S. nexus, particularly for non-U.S. subsidiaries of U.S. companies, while also explaining the important changes brought about under the JCPOA.

Enduring U.S. extraterritorial sanctions risk under the JCPOA

The baseline point to understand is that the ITSR, which are administered by the U.S. Treasury Department's Office of Foreign Assets Control ('OFAC'), generally apply only to 'U.S. Persons', which does not include companies organised under the laws of a non-U.S. jurisdiction. The definition of 'U.S. Persons' under OFAC's ITSR covers U.S. citizens or lawful permanent residents, wherever located; entities organised under the laws of a U.S. jurisdiction, including their foreign branch offices; and any person or entity located in the United States. So a non-U.S. company's facility in the United States would be treated as a U.S. Person, as would a U.S. company's unincorporated facility abroad. Entities based and located outside the United States, however, are not U.S. Persons under the ITSR, even if 100% owned and fully controlled by a U.S. Person. Thus, prior to the end of 2012, the general rule was that non-U.S. subsidiaries of U.S. companies were not directly subject to the ITSR or most OFAC sanctions (with OFAC's Cuba sanctions, issued under the Trading With The Enemy Act, being an exception).

However, in 2012, the U.S. Congress required OFAC to extend the ITSR to transactions conducted 'knowingly' by entities 'owned or controlled' by U.S. Persons. So even though non-U.S. subsidiaries were (and are) not 'U.S. Persons', as of 26 December 2012, such entities were made subject to the ITSR, essentially as if they were 'U.S. Persons'. The JCPOA then required the

United States to undo this expansion of the ITSR's jurisdictional reach, at least in part. To satisfy the U.S. obligation under the JCPOA, on 16 January 2016, the U.S. government took two major steps: (1) 'secondary sanctions' directed at non-U.S. Persons that are not affiliated with U.S. Persons were largely (but notably, not fully) suspended, and (2) OFAC published General License H, authorising non-U.S. entities 'owned or controlled' by U.S. Persons to engage in transactions with Iran and the government of Iran that were prohibited under the ITSR, provided that certain limitations are observed. So while non-U.S. subsidiaries remain subject to the ITSR under the 2012 expansion, General License H provides an authorisation that overrides the prohibitions in many instances. The following discussion focuses on the risk points non-U.S. Persons must address before going into Iran – those arising from the JCPOA changes as well as those that have persisted since 1995.

First, when non-U.S. Persons – whether or not subsidiaries of U.S. companies – plan to do business involving Iran, no 'U.S. Persons' can 'facilitate', 'approve' or 'guarantee'that non-U.S. Person activity if the ITSR would otherwise prohibit a U.S. Person from engaging in that same activity. There are some narrow exceptions, such as OFAC allowing U.S. Persons to conduct legal compliance reviews of the proposed business (e.g., of a non-U.S. subsidiary) or providing 'informational-materials' in support of the transaction. And OFAC's view of what is improper 'facilitation' or 'approval' is quite broad, undefined, and subject to the discretion of the agency – not very comforting from a business planning perspective.

This restriction on facilitation or approval applies to U.S. Person expatriate officers, directors or employees, as well as many other structural business links to the United States. It applies even if the non-U.S. Person's business might be otherwise totally lawful for the non-U.S. Person to pursue. In other words, U.S. Persons essentially cannot be involved in any activity that is prohibited under the ITSR, even if the primary actor is not subject to the ITSR or is otherwise authorised under General License H.

U.S. Person involvement

What are the risks if a non-U.S. Person were either deliberately or even accidentally to involve a U.S. Person? Well, the U.S. Person could be subject to civil or criminal penalties. The non-U.S. Person could be charged with aiding or abetting a violation, conspiring to commit a violation, 'causing' (under a 2007 amendment to the International Emergency Economic Powers Act) a violation of U.S. law, or indeed with exporting U.S.-origin 'services' (in the form of the U.S. Person's involvement) to Iran. Non-U.S. banks that involved U.S. banks in funds transfers originating from Iran (and other U.S.-sanctioned countries) found themselves on the other end of civil and criminal penalties, some as large as billions of dollars, over the past eight years – apparently on one or more of these theories of liability.

It is clear that linkages with U.S. Person individuals or U.S. goods or service suppliers can present risks to non-U.S. Persons who do business with Iran. Such linkages need to be assessed in advance of actual business by non-U.S. companies (even including entering into contracts) to determine if the enforcement risks noted above are acute, non-existent, or manageable.

Sourcing risks

Another risk under the ITSR for non-U.S. Persons, including non-U.S. subsidiaries of U.S. companies, is sourcing goods, services, software or technology (collectively, 'items') from the United States for purposes of conducting business with Iran. Since the U.S. government has largely maintained the ITSR sanctions 'as is', despite the JCPOA, one specific provision of those primary sanctions does directly apply to non-U.S. Persons, including non-U.S. subsidiaries. Section 560.205 explicitly prohibits non-U.S. Persons from engaging in trade or other business transactions with Iran, if that activity would involve the export or supply of items 'subject to' U.S. export control jurisdiction – which includes U.S. origin items as well as non-U.S. origin items that contain more than 10% U.S. controlled content or are produced from certain U.S. technology. Items of U.S. origin create a potentially enduring link to U.S. regulatory and enforcement jurisdiction under the ITSR, as well as under U.S. export control regulations. This is true even when U.S. Persons may not be the actual suppliers of the item subject to U.S. jurisdiction. U.S. origin items may already be abroad when they are acquired by a non-U.S. Person for sale to Iran, but their U.S. origin can still give rise to U.S. jurisdiction. Of course, there are situations in which U.S. sourcing may be proper, but any U.S. supply chain linkage creates risks that need to be evaluated. This includes what might be called services that relate to the commercial feasibility of any transaction, such as banks, insurers, carriers, freight forwarders, and other logistics providers.

Non-U.S. Persons are still at risk of certain secondary sanctions, even without a U.S. nexus, if they engage in certain trade, investment, financial, or other business activity involving Iran.

In addition, non-U.S. companies should be aware that OFAC can add them to its list of Specially Designated Nationals and Blocked Persons ('SDNs') for providing material support to other SDNs, among other possible triggers. While the general provision for material support designations for Iran (Executive Order 13645) has been repealed as part of the JCPOA, providing material support to SDNs may still be sanctionable under other executive orders – this has been a common source of confusion. SDN designation risk is complex and has been further complicated under the JCPOA; while it is not the focus of this article, it is something to remain aware of.

Finally, non-U.S. Persons are still at risk of certain secondary sanctions, even without a U.S. nexus, if they engage in certain trade, investment, financial, or other business activity involving Iran. For example, if a non-U.S. Person were to engage in a significant transaction (not clearly defined) with a specified list of SDNs, the Iranian Revolutionary Guard Corps or its agents or affiliates, or those

engaged in certain illicit behaviour (such as terrorism, WMD activity, human rights abuses, or destabilising conduct in Syria or Yemen), that non-U.S. Person can suffer market access limitations, such as being cut off from the U.S. financial system, blacklisted from doing business with U.S. Persons, cut off from U.S.-licensed export transactions, Ex-Im Bank financing, and so on.

A U.S. Person's self-recusal [from sanctioned country activity] can itself be treated as a prohibited act of facilitation, or 'evasion', particularly if it allows sanctioned country business to move forward.

In the sections that follow, we discuss three of the practical challenges that continuing U.S. sanctions on Iran present for non-U.S. companies: (1) how to handle U.S. expatriate personnel; (2) how much support a U.S. parent company or other U.S. entities can offer; and (3) U.S. supply chain risks.

U.S. expatriates

U.S. citizens and permanent resident aliens (so-called 'green card' holders) are widely present throughout the international business community, but it is not commonly understood that these individuals are themselves subject to U.S. sanctions jurisdiction. Moreover, a non-U.S. company may even be held vicariously liable for the acts of its U.S. Person employees acting within the scope of their duties, although the precise scope of that potential jurisdiction is not clear when the non-U.S. company itself would not be subject to U.S. jurisdiction for the same activity. For example, if a U.S. Person working for a French company is involved in unlawfully exporting a U.S. origin item to Iran, both the U.S. Person individual and the non-U.S. company could be held liable. If the involvement of the U.S. Person pertains to a non-U.S. Person's offshore transaction that does not otherwise involve the U.S. economy, the U.S. Person can still be held liable, and the non-U.S. Person company should be concerned if there is evidence of conduct that 'caused' the U.S. Person expat to violate the law. A U.S. Person, who is a member of the board of directors, senior officer, controlling shareholder, key employee, or long-term contractor, is subject to OFAC's jurisdiction anywhere in the world and can be liable for facilitation. These risks have not gone away under the JCPOA, and remain highly relevant for any non-U.S. company considering entering (or re-entering) the Iran market.

Recusal of U.S. Persons from sanctioned country activity can reduce U.S. legal risk, but a U.S. Person's self-recusal can itself be treated as a prohibited act of facilitation, or 'evasion', particularly if it allows sanctioned country business to move forward, such as in a board vote. Recusal can be complex to implement safely. There are other ways in which U.S. Persons can get themselves and their companies into trouble, even when trying to be compliant. For example, a U.S. Person cannot simply delegate his or her responsibility for sanctioned country business: OFAC may consider that to be a prohibited referral of business to the delegatee and treat it as unlawful facilitation or evasion. The bottom line is that companies dealing in sanctioned countries with any involvement by U.S. Persons are subject to a high level of risk. There may be solutions, but even the solutions can be minefields. This is an area that should be approached with great caution.

Support from U.S. Parents or other U.S. entities

This is one area in which the JCPOA does offer some relief. OFAC's General License H, issued pursuant to the JCPOA, sets out two narrow exceptions to the facilitation prohibition discussed above by authorising U.S. Persons to engage in the following activities that would otherwise be prohibited: '(1) activities related to the establishment or alteration of operating policies and procedures of a United States entity or a U.S.-owned or -controlled foreign entity, to the extent necessary to allow a U.S.-owned or -controlled foreign entity to engage in transactions [in Iran]; and (2) activities to make available to those foreign entities that the U.S. Person owns or controls any automated [i.e. operating "passively and without human intervention" – or at least without human intervention in the United States] and globally integrated [i.e. "available to, and in general use by," the "global organization"] computer, accounting, email, telecommunications, or other business support system, platform, database, application, or server necessary to store, collect, transmit, generate, or otherwise process documents or information related to transactions [with Iran].'

As those two exceptions in General License H are still quite new, their precise contours are still being defined, and companies would be well-advised to act cautiously in light of the broad underlying prohibition on facilitation that remains in effect. Typically, OFAC construes general licences cautiously, although this is a unique situation in which the United States is subject to a treaty obligation in the JCPOA to 'license non-U.S. entities that are owned or controlled by a U.S. Person to engage in activities with Iran that are consistent with this JCPOA'. The U.S. government has an obligation to implement that commitment in a good faith manner, and without being unduly restrictive. Even so, OFAC is likely to adhere closely to the text and underlying purpose of the two exceptions in General License H.

OFAC's Frequently Asked Questions make clear that General License H does not authorise U.S. Persons to become involved in 'ongoing' or 'day-to-day' Iran-related operations or decision making, including by approving, financing, facilitating, or guaranteeing any Iran-related transaction by a non-U.S. entity. U.S. Persons can only get involved in the 'initial determination' to engage in the limited set of activities in Iran not excluded by General License H and the 'establishment or alteration of the necessary policies and procedures', along with providing training on these policies and procedures. U.S. Person facilitation activity that may exceed these parameters presents risk that needs to be assessed – which raises the question: What does the facilitation provision generally require in order to remain within the law when a subsidiary is operating in a sanctioned country?

As a best practice to avoid being charged with facilitation, U.S. parent

companies must ensure that their foreign subsidiaries or affiliates act independently of any U.S. Person when engaged in specific sanctioned country activity, including in areas such as business and legal planning; decision making; designing, ordering or transporting goods; and financial, insurance, and other aspects of the specific business opportunity with Iran.

In addition, U.S. Persons can be charged with unlawful facilitation for referring business opportunities with sanctioned countries or entities to non-U.S. Persons. Other than the special circumstances of the Iran programme and General License H specifically, OFAC still prohibits U.S. companies from changing their own policies or operating procedures, or those of their subsidiaries, in order to 'enable' a subsidiary to enter into a transaction that would be prohibited for a U.S. Person.

While this paints a broad picture of the facilitation prohibition, there are certain types of support to foreign subsidiaries engaged in sanctioned country business that may not be prohibited. For example, OFAC's Sudanese Sanctions Regulations specify that facilitation does not include '[a]ctivity of a purely clerical or reporting nature that does not further' prohibited transactions, such as 'reporting on the results of a subsidiary's trade' with a sanctioned country or person.[2] On the other hand, financing or insuring that trade, or warranting the quality of goods, would constitute prohibited facilitation. There is much that falls between these two bookends – activity 'of a purely clerical or reporting nature' and things like financing – but a potential rule of thumb is that U.S. parent companies will typically not be prohibited from providing generic administrative support to their subsidiaries that is not specific to sanctioned country activity, does not 'further' or 'enable' that activity in and of itself, and does not compromise the 'independence' of the subsidiary with respect to that activity. So, for example, if a foreign subsidiary of a U.S. company uses the U.S.-based email server to correspond with Iranian customers, that would not seem to be the type of U.S. Person facilitation OFAC had in mind, as long as the email server function is generally the same for all activities of the foreign subsidiaries, and no U.S. Persons are pulled into those specific email communications to assist in the transaction or marketing effort of the foreign subsidiary. But, given the inherent ambiguity of the sanctions regulations, and the underlying objective to forbid U.S. Person involvement, each situation, even when relating only to generic, administrative support, warrants careful consideration.

U.S. parent companies must ensure that their foreign subsidiaries or affiliates act independently of any U.S. Person when engaged in specific sanctioned country activity.

Certain corporate structures present particularly complex risk in this area, such as companies that largely operate overseas, but that have management, legal, commercial or other kinds of support provided from the United States. Two recent criminal cases illustrate this type of structural risk. The first involved Switzerland-based Weatherford International Ltd., which was charged for, among other things, concealing transactions with Iran conducted through a Dubai subsidiary by referring to Iran as 'Dubai across the waters', and in other instances concealing the U.S. origin of the items it was selling.[3] Weatherford had issued policies prohibiting sanctioned country business, but its U.S.-based executives in practice allegedly supported and directed this business by the foreign subsidiaries. So even though Weatherford was based in Switzerland, its U.S.-based executives brought its activities under U.S. jurisdiction.

In the second case, Schlumberger Oilfield Holdings Ltd. ('SOHL') pled guilty to a conspiracy charge for transactions with Iran and Sudan.[4]

SOHL was a non-U.S. subsidiary of Schlumberger Ltd., a Curaçao (Netherlands) entity with headquarters in the United States, the Netherlands and France. In other words, the charges were against a non-U.S. subsidiary of a non-U.S. company that based some of its management and support personnel in the United States (some of whom were not even U.S. citizens or permanent residents). It was the actions of those U.S.-based personnel that triggered U.S. jurisdiction and the charges against SOHL for 'conspiring' with them to conduct trade with Iran and Sudan. Like Weatherford, Schlumberger had developed concealment schemes like calling Iran the 'Northern Gulf'.

What may be most remarkable about the Weatherford and Schlumberger cases is that they do not appear to turn on the fact that the U.S.-based personnel supporting the sanctioned country business were part of the company. A conspiracy with a U.S. Person could therefore potentially involve an unaffiliated service provider in the United States, or possibly even things like technical support (the Schlumberger case involved technical support as well as U.S.-based management). These cases could be said to set out the broad legal principle that non-U.S. companies operating outside the United States can be held liable under U.S. law for business with sanctioned countries or persons whenever that activity involves a U.S. Person, wherever located, or any person or entity located in the United States, acting on behalf of the company and within the scope of their duties. The U.S. Person can be charged with facilitation, among other things, and the non-U.S. company can be charged with conspiracy, causing a violation, or aiding and abetting, among a litany of other possible charges.

U.S. supply chain risks

Dealing with U.S.-origin items can often be the most challenging risk for non-U.S. companies to manage, as U.S. jurisdiction can follow those items and all of the individuals and companies that deal with them, anywhere in the world. The trickiest part is that it is not just completed end-items that trigger U.S. jurisdiction, but even fairly minor components, software and underlying technologies can have that effect. U.S. law broadly prohibits exports of goods, services, software, or technology from the United States or by U.S. Persons, directly or indirectly, to Cuba, Iran, Sudan, Crimea, North Korea and Syria. The U.S. also generally prohibits re-exports (i.e., shipments from a third country) to these sanctioned destinations of items that are of U.S. origin or contain more than a *de minimis* amount (10% for most sanctioned countries) of U.S.-origin controlled content. This area is complex, with some of the sanctions programmes applying somewhat different rules, and also requiring an analysis of U.S. export control regulations.

Non-U.S. companies operating outside the United States can be held liable under U.S. law for business with sanctioned countries or persons whenever that activity involves a U.S. Person.

For Iran, OFAC prohibits: (1) imports of most Iranian goods or services; (2) exports and re-exports to Iran of most goods, technology or services from the United States or by a U.S. Person anywhere in the world; and (3) exports or re-exports to a third country with reason to know that the items are intended specifically for Iran. For non-U.S. persons, trade with third countries intended specifically for Iran is only prohibited when the items were exported from the United States and controlled under U.S. export control regulations.

These prohibitions largely remain in place under the JCPOA, with a limited new (in fact, restored) authorisation for imports of Iranian-origin carpets and foodstuffs, and a newly enacted policy (or significant expansion of the pre-existing policy, which only related to aircraft safety) allowing companies to seek case-by-case approval for exports and re-exports of commercial passenger aircraft and related parts and services. There are also pre-existing authorisations allowing exports or re-exports to Iran of certain types of food, agricultural commodities, medicine and medical supplies, as well as informational materials, certain services and software related to Internet-based communications, certain services, software, and hardware incident to personal communications, and certain other goods and services.

As OFAC prohibits most trade with Iran that has a U.S. nexus, non-U.S. companies, whether or not affiliated with a U.S. owner, should try to understand the myriad ways they can

Links and notes

[1] Some refer to these as 'extraterritorial' measures, because they often have the effect of extending OFAC's sanctions to non-U.S. Persons acting outside the United States. Others disagree with the use of that term, because these measures are still so-called 'primary' sanctions, in that they are prohibitions enforceable against the target itself, as opposed to 'secondary' sanctions, which are enforceable against U.S. Persons that the target may deal with.

[2] The description of the facilitation prohibition in this paragraph and the next is based on OFAC's Sudanese Sanctions Regulations, 31 C.F.R. § 538.407. Many practitioners agree that OFAC tends to apply concepts such as this across its sanctions programmes, so this Sudan provision is relevant to the scope of the facilitation prohibition for Iran. Some of OFAC's regulations, like Cuba for example, do not even mention facilitation. But it is clear that, in practice, OFAC has applied that prohibition in its Cuba regime. The Iran regulations also elaborate on the facilitation provision, but not to the same extent as the Sudan regulations. C.f. 31 C.F.R. § 560.417.

[3] See, e.g., In the Matter of Weatherford International Ltd. Et al., , U.S. Dep't Of Commerce, Bureau Of Industry And Security, (Dec. 23, 2013) http://efoia.bis.doc.gov/index.php/component/docman/doc_download/921-e2353-r?Itemid=.

[4] See, e.g., Plea Agreement *United States v. Schlumberger Oilfield Holdings, Ltd.*, U.S. Department of Justice (March 24, 2015), http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/25/schlumberger_plea_agreement.pdf.

[5] KMT Group AB Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations, U.S. Dep't of The Treasury, Office Of Foreign Assets Control (25 October 2013), https:// www.treasury.gov/resource-center/sanctions/CivPen/

Documents/20131025_kmt.pdf (stating that CBP seized the items upon redelivery from Europe to the United States).

[6] Thermon Manufacturing Company Settles Sudanese Sanctions Violation Allegations, U.S. Dep't Of The Treasury, Office of Foreign Assets Control (31 August 2009), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/ Documents/09012009.pdf; In the Matter of Thermon (U.K.) Ltd., U.S. Dep't Of Commerce, Bureau of Industry And Security (Sept. 11, 2009), http://efoia.bis.doc.gov/index.php/component/docman/doc_view/523-e2131?Itemid=

find themselves caught up in these rules: they may export from the United States; they may deal in goods that have more than 10% U.S.-origin controlled content or that are the 'direct product' of certain U.S. technologies; or they may have facilities in the United States for which they import Iranian-origin goods or use Iranian services, among other risks. For most international companies, it is not practical to try to remain in a position involving no U.S. jurisdiction at all, given how far-reaching it can be. And this risk is not merely theoretical – both OFAC and the U.S. Commerce Department's Bureau of Industry and Security ('BIS') are active in pursuing enforcement actions against both U.S. and non-U.S. companies.

Most of OFAC's enforcement actions in the supply chain area have involved indirect exports from the United States through third countries. This may be explained in part by the fact that many of OFAC's trade-based cases start with seizures or tips by U.S. Customs and Border Protection ('CBP'). But OFAC and BIS have clear authority to bring other types of cases as well, such as direct re-exports of U.S.-origin items from third countries to Iran. Enforcement, in practice, can stem from a variety of risk areas, including, for example, return of goods to the United States for repair or replacement, which appears to have been how Sweden-based KMT Group AB came under investigation in 2013.[5]

Another good example is U.S.-based Thermon Manufacturing Co., which settled charges by OFAC, along with BIS charges against several of its non-U.S. subsidiaries, for shipping goods to sanctioned countries.[6] This case is a cautionary tale for U.S.-based companies that do not conduct enough oversight and due diligence to prevent subsidiaries from concealing unlawful transactions. BIS charged Thermon U.K., for example, with causing and aiding and abetting violations by its U.S. parent for, among other things, placing orders with the parent for items shipped through the U.K., without informing the parent that the items were destined for Iran. The U.S. parent company had issued instructions to its subsidiaries prohibiting them from selling to sanctioned countries, but those instructions were not effective, and no fault is required in these strict-liability regulatory regimes.

Conclusion

The takeaway from all of this is that non-U.S. companies will continue to face risks in dealing with Iran, even under the JCPOA, when they are U.S.-owned or controlled, have U.S. expatriate personnel, use an international supply chain, have U.S.-based managers or obtain other significant support from the United States. From a big picture perspective, the nuclear deal with Iran has not eliminated these risks, and non-U.S. companies would be well served by exercising great caution as they decide to re-enter the Iran market.

Ed Krauland is a partner and Peter Jeydel is an associate at the Washington, DC office of international law firm Steptoe & Johnson LLP.

ekrauland@steptoe.com

pjeydel@steptoe.com

THE WORLDECR EXPORT CONTROLS AND SANCTIONS FORUM 2016

LONDON

Official sponsors

GvW Graf von Westphalen

BRAUMILLER LAW GROUP, PLLC INTERNATIONAL TRADE LAW

Hogan Lovells

Dechert LLP

Amber Road POWERING GLOBAL TRADE

Official evening reception sponsor

Debevoise & Plimpton

13-14 OCTOBER, 8 FENCHURCH PLACE, LONDON EC3 ● VISIT WWW.WORLDECR.COM FOR DETAILS

North Korea sanctions

U.S. economic sanctions on North Korea in 2016 and why you should care (particularly non-U.S. companies)

The U.S. government has imposed secondary sanctions on non-U.S. person trade with North Korea, similar to 2010 secondary sanctions imposed on Iran. Kay Georgi, Regan Alberda and Julia Diaz examine the developments.

Although the United States has had effective economic sanctions on North Korea for many years, the temporary softening of US sanctions in 2000 has given way to ever-increasing sanctions since 2008. These U.S. sanctions are not unilateral: the United Nations has also increased the list of sanctioned individuals in North Korea, banned all weapons trade with the country, and required countries to inspect all cargo going in or out of North Korea to ensure no contraband is being transported.

So why did the world take notice when the U.S. government put North Korean leader Kim Jong Un and other North Korean officials and entities on the Specially Designated Nationals ('SDN') list on 6 July 2016?

Well, it's always a big deal when the U.S. government places another country's leader on the SDN list. Others who have been placed on the list include Robert Mugabe (Zimbabwe) and Saddam Hussein (Iraq). North Korea is not happy about the sanctions, calling them tantamount to a declaration of war and cutting off its only diplomatic communication channel with the United States (a United Nations channel in New York).

What's more, the 6 July designations are just the latest in a series of efforts by the U.S. in 2016 to curb North Korea's human rights abuses and nuclear ambitions. During the first half of 2016, the U.S. government has enacted and signed a law authorising the imposition of sanctions on North Korea and issued two executive orders expanding on those sanctions.

An examination of the newly enacted laws and executive orders shows how the U.S. has opened the door to secondary sanctions on non-U.S. person trade with North Korea.

These new laws and executive orders have enabled the U.S. government to impose secondary sanctions (those that apply to non-U.S. persons outside the U.S. on wholly non-U.S. conduct of business with North Korea), in a manner resembling how the U.S. government imposed secondary sanctions on Iran beginning in 2010 with The Comprehensive Iran Sanctions, Accountability, and Divestment Act ('CISADA') and expanding in 2012 with the Iran Threat and Syria Human Rights Act ('ITRSHA'), as well as other statutes and numerous executive orders.

An examination of the newly enacted laws and executive orders shows how the U.S. has opened the door to secondary sanctions on non-U.S. person trade with North Korea:

E.O. 13687 (2 January 2016)

- Authorises OFAC to designate and block the assets of agencies, instrumentalities and controlled entities of the government of North Korea and the Workers' Party of Korea, and officials of the government of North Korea and the Workers' Party of Korea that come into the possession or control of U.S. persons.
- Also authorises OFAC to block the assets of persons OFAC determines 'have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the government of North Korea or any person whose property and interests in property are blocked' pursuant to the order.

The 'North Korea Sanctions and Policy Enhancement Act of 2016' (signed into law on 19 February 2016)

- Extends the previously implemented ban on exports to North Korea to include all goods and technology exports as laid out in section 6(j) of the Export Administration Act of 1979 (50 U.S.C. 4605).
- Expands asset-blocking rules to include entities owned or controlled, or acting on behalf of a designated person, rather than entities owned 50% or more by one or more SDNs (as was previously the rule). For a list of currently blocked persons or entities, please see OFAC's SDN List.
- In section 104(a), increases mandated (not discretionary) North

Links and notes

6 July designations
https://www.treasury.gov/press-center/press-releases/Pages/jl0506.aspx?utm_source

Executive Order 13687
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13687.pdf?utm_source

Section 6(j) of the Export Administration Act of 1979 (50 U.S.C. 4605)
http://legcounsel.house.gov/Comps/eaa79.pdf?utm_source

Executive Order 13722
https://www.treasury.gov/resource-center/sanctions/Programs/Documents/nk_eo_20160316.pdf?utm_source

Korea-related primary and secondary sanctions (those that apply to non-U.S. persons outside the U.S.) to require OFAC to designate any person who breaches certain prohibitions, including knowingly:
(1) Importing or exporting banned items relating to nuclear proliferation, chemical and biological weapons, and missile technology;
(2) Providing training, advice, or other assistance, or engaging in significant financial transactions, concerning items relating to nuclear proliferation, chemical and biological weapons, and missile technology;
(3) Importing, exporting, or re-exporting luxury goods;
(4) Facilitating censorship by the government of North Korea;
(5) Facilitating serious human rights abuses by the government of North Korea;
(6) Engaging in money laundering, counterfeiting of goods or currency, bulk cash smuggling, or narcotics trafficking that supports the government of North Korea;
(7) Engaging in significant activities undermining cybersecurity through the use of computer networks or systems against foreign persons, governments, or other entities on behalf of the government of North Korea
(8) Selling, supplying, or transferring to or from the government of North Korea (or any person acting on its behalf) a significant amount of precious metal, graphite, raw or semi-finished metals or aluminium, steel, coal, or software, for use by or in industrial processes directly related to weapons of mass destruction and their delivery systems, other proliferation activities, the Korean Workers' Party, armed forces, internal security, or intelligence activities, or the operation and maintenance of political prison camps or forced labour camps, including outside North Korea;
(9) Importing, exporting, or reexporting arms or related materiel; or
(10) Knowingly attempting to engage in any of the conduct described in paragraphs (1) to (9).

- In section 104(b), authorises the following discretionary sanctions to allow OFAC to designate any person who breaches certain prohibitions, including knowingly:
(1)(A) Engaging in, contributing to, assisting, or providing support to, any SDN;
(1)(B) Contributing to (i) the bribery of an official of the government of North Korea or someone working on their behalf; (ii) the misappropriation, theft, or embezzlement of public funds by, or for the benefit, of, an official of the government of North Korea or someone working on their behalf; and (iii) using the proceeds of any activity described in (i) or (ii).

E.O. 13722 (15 March 2016)

- Implements the North Korea Sanctions and Policy Enhancement Act of 2016.
- In section 2(a), expands on the North Korea Sanctions and Policy Enhancement Act of 2016 to authorise OFAC to designate and block the property of persons determined by OFAC as follows:
(i) To operate in any industry in the North Korea economy as may be determined by the Secretary of Treasury, in consultation with the Secretary of State, to be subject to this subsection, such as transportation, mining, energy, or financial services;
(ii) To have sold, supplied, transferred, or purchased, directly or indirectly, to or from North Korea or any person acting for or on behalf of the government of North Korea or the Workers' Party of Korea, metal, graphite, coal, or software, where any revenue or goods received may benefit the government of North Korea or the Workers' Party of Korea, including North Korea's nuclear or ballistic missile programmes;
(iii) to have engaged in, facilitated, or been responsible for an abuse or violation of human rights by the government of North Korea or the Workers' Party of Korea or any person acting for or on behalf of either such entity;
(iv) to have engaged in, facilitated, or been responsible for the exportation of workers from North Korea, including exportation to generate revenue for the government of North Korea or the Workers' Party of Korea;
(v) to have engaged in significant activities undermining cyber-security through the use of computer networks or systems against targets outside North Korea on behalf of the government of North Korea or the Workers' Party of Korea;
(vi) to have engaged in, facilitated, or been responsible for censorship by the government of North Korea or the Workers' Party of Korea;
(vii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this order;
(viii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or
(ix) to have attempted to engage in any of the activities described in subsections (a)(i)–(viii) of this section.
- Prohibits all exports and re-exports of goods, services and technology from the United States or by U.S. persons, new investment in North Korea by U.S. persons, and approval or facilitation by U.S. persons of foreign person actions with respect to North Korea that would be prohibited for a U.S. person.

The 6 July 2016 SDN designations expand the SDN List to include several North Korean top officials, including North Korean leader Kim Jong Un.

6 July 2016 SDN designations

- Expands the SDN List to include several North Korean top officials, including North Korean leader Kim Jong Un, ten other individuals, and five entities. The designations were issued pursuant to E.O. 13722 and E.O. 13687, and were made in conjunction with the State Department's release of its 'Report on Serious Human Rights Abuses or Censorship in North Korea.'

The SDN List now includes all of the individuals and entities named in the State Department's report.

Secondary sanctions are coming

The combined effect of the two recent executive orders, plus the North Korea Sanctions and Policy Enhancement Act of 2016, is to allow the U.S. Department of Treasury, in coordination with U.S. Department of State, to impose sectoral SDN or other sanctions on non-U.S. companies operating in the North Korean transportation, mining, energy, or financial services sectors. OFAC is also able to designate as SDNs non-U.S. persons who have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to, or in support of, the government of North Korea and SDNs. Less surprisingly, persons who have provided support to North Korea's nuclear or ballistic missile programme, who have facilitated or engaged in human rights abuses or violations, who have exported workers from North Korea, who have engaged in undermining cybersecurity on behalf of the North Korea government, or who have engaged in or facilitated censorship in North Korea, can also be designated.

Non-U.S. companies doing business in market areas where North Korea produces, for example, should consider extra due diligence that the products they are trading are not of North Korean origin.

In short, North Korea in many ways is stepping into Iran's shoes as a potential source of secondary sanctions for non-U.S. companies providing material support to the North Korean regime or, in the future, operating in certain North Korean sectors. Non-U.S. companies doing business in market areas where North Korea produces, for example, should consider extra due diligence that the products they are trading are not of North Korean origin. Similarly, companies selling to resellers or other intermediaries should take care to know the ultimate customer. This task is made substantially more difficult by the blocking of entities owned or controlled, or acting on behalf of by a designated person, rather than merely entities owned 50% or more by one or more SDNs.

Kay Georgi is a partner, Regan Alberda is counsel, and Julia Diaz is an associate in the Washington, DC office of Arent Fox.

kay.georgi@arentfox.com

regan.alberda@arentfox.com

julia.diaz@arentfox.com

UK/EU encryption – what is controlled?

Encryption is the tool of choice for ensuring security of data, and controls on exports of cryptographic items are wide-ranging. Richard Tauwhare reviews current UK and EU export controls on encrypted items and asks where next for the controls as they race to keep up with developments in this ever-changing field.

Data protection, cybersecurity, commercial confidentiality and personal privacy all demand high standards of security for data stored or transmitted electronically. The primary means to achieve this is encryption. But this can be misused for military, criminal or terrorist purposes. Exports of many cryptographic items are therefore subject to export controls, including many that are widely used in everyday commercial applications. Although the rules are essentially the same across the EU and in the U.S., their interpretation varies widely and many businesses struggle to implement them correctly. What is controlled, what is exempt, what licences are available and what is changing?

What is controlled?

All products capable of encrypting data, regardless of any other functions they may have, may be subject to export controls. Current EU and U.S. regulations in principle require an export licence for all products using symmetric algorithms with a key length over 56 bits or asymmetric algorithms with a key length over 512 bits. But many commonly used encryption protocols now use key lengths exceeding these levels (e.g. AES 128, 1024 RSA, 1024 DH). All such products are in principle subject to export restrictions.

This is not restricted to hardware but includes components, electronic assemblies, software and technology. Phones, computers and tablets that contain product design data or software are also subject to licence restrictions if carried outside the EU. And since the definition of export includes the transmission of software or technology by any electronic means, even if the data is encrypted, the current EU interpretation is that allowing overseas access to the encrypted data is still an export, including read access to software (object code as well as source code).

All information security items subject to export controls in the EU are listed in Category 5 Part 2 of Annex I of the EU Dual-Use Regulation (Council Regulation (EC) 428/2009). All items on the list require a licence for export outside the EU, unless they qualify for an exemption (or 'de-control').

What is exempt?

The regulators have increasingly had to recognise that cryptographic products that only a few years ago were reserved to only the most sophisticated commercial users and government agencies are now commonplace on every smartphone and wireless router. In order to enable unrestricted trade in the highly competitive market for such commercial products while retaining effective control of more sensitive items, the regulations agreed internationally in the Wassenaar Arrangement and adopted into law by most major exporting countries including the EU allow for significant exemptions. These fall under ten main headings:

1) Software 'in the public domain' – defined as software that has been made available without restrictions (excluding copyright restrictions) upon its further dissemination. This generally exempts open source software, including that made available under a licence from the copyright holder.
2) There is a general exclusion for controlled components once they have been incorporated into a non-controlled product unless the components are 'the principal element of the goods and can feasibly be removed for other purposes'.
3) Although there is a general

exemption for software and technology which is the minimum necessary for the installation, operation, maintenance (checking) or repair of goods that are not controlled or whose export has already been authorised, it is important to note that this does not apply to information security software controlled in Category 5 Part 2, i.e. cryptographic software.

4) Cryptographic products whose sole function is authentication (i.e. encryption directly related to the protection of passwords, PINs or similar data to prevent unauthorised access), digital signatures or the execution of copy-protected software, including their associated key management functions.
5) Smart cards and smart card reader/writers if they are either specially designed to protect personal data (linked to the exemption for authentication items above) or if they are excluded from controls by 'Note 4' (see below).
6) A list of commonly used commercial cryptographic equipment including that used for banking or money transactions; most civil mobile phones; cordless phones; short range wi-fi equipment; civil Radio Access Network equipment; routers, switches and relays limited to Operations, Administration or Maintenance ('OAM') functions; and certain general purpose computing equipment and servers using only published or commercial cryptographic standards.
7) Listed information security items are not subject to export controls 'when accompanying their user for the user's personal use' ('Note 2').
8) A broader category of exemptions is set out in the 'Cryptography Note'. This exempts consumer-type products that can be purchased by the general public ('Note 3a'). To be exempt, an item must meet all of the following six conditions:
   a) generally available to the public by being sold, without restriction (except for those normally arising from copyright), from stock at retail selling points (e.g. high street shops, e-commerce) by means of any of the following transactions: over-the-counter, mail order, electronic or telephone call;
   b) the cryptographic function cannot easily be changed by the user;
   c) designed for installation by the user without further substantial support by the supplier;
   d) when necessary, details of the goods are accessible and will be provided upon request to the competent authorities of the Member State in which the exporter is established in order to ascertain compliance with the conditions above;
   e) the item is of potential interest to a wide range of individuals and businesses; and the price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier.

All products capable of encrypting data, regardless of any other functions they may have, may be subject to export controls.

In determining eligibility for exemption, the regulator may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier. Interpreting and applying the Cryptography Note is notoriously difficult: this is discussed further in the next section.

9) Hardware components or executable software that have been designed for existing items described above ('Note 3b'). This is aimed at items that are to be incorporated into specific products exempted above but which are not necessarily available to the general public. To qualify for exemption, such an item needs to meet all of the following conditions:
   a) Information security is not its primary function or set of functions;
   b) It does not change or add any cryptographic functionality to the existing items;
   c) Its feature set is fixed and is not designed or modified to customer specification; and
   d) When necessary as determined by the competent authorities of the Member State in which the exporter is established, its details and details of relevant end-items are accessible and will be provided to the competent authority upon request, in order to ascertain compliance with conditions.
10) Finally, items incorporating or using cryptography are exempt if they meet all of the following conditions ('Note 4'):
   a) the primary function or set of functions is not any of the following:
      - Information security;
      - A computer, including operating systems, parts and components therefor;
      - Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or
      - Networking (includes operation, administration, management and provisioning);
   b) The cryptographic functionality is limited to supporting their primary function or set of functions; and
   c) When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described above.

How are these exemptions applied?

While the majority of these exemptions or de-controls are relatively straightforward, there are significant differences between regulators in their

interpretation and application of exemptions in the Cryptography Note: the U.S. is less restrictive than most EU Member States, which in turn are less restrictive than the UK. In the UK, the exemption is in practice permitted only to a small number of low-price, high-volume products purchased from high street stores or online, only for home or small business users. This is causing serious challenges, in particular:

- The UK's restrictive position does not in practice provide effective control of the goods it regards as higher risk since many of these are freely available from the U.S. as well as from some other EU states. The UK's position merely restricts UK trade and creates additional workload for the UK Export Control Organisation ('ECO') and industry through additional licensing;
- Companies that operate in the EU may wrongly assume that because an export licence for a specific item is not required in the U.S., an EU licence is not required either. That can, for example, be the case for products that come under the U.S. ECCNs (Export Control Classification Numbers) 5A992 or 5D992 i.e. waived a U.S. licence requirement because the item is considered 'mass market' but for which no equivalent classification exists in the EU. This can lead to EU companies breaching export control regulations by exporting such items from the EU without a licence;
- Some EU regulators, particularly in the UK, interpret the exemptions in a highly subjective way and provide little guidance on how they apply the rules, making it difficult for exporters to classify items for themselves. This is resulting in companies who decide that a particular item does not require a licence having their goods held at the border while the customs authorities confirm with the ECO whether an export licence is required. At best, this causes minor delays, but, if the regulator decides that a licence is required, there can be a substantial delay while a licence is obtained, and the exporter risks facing enforcement action for breaching export control regulations.

As a result some companies, particularly in the UK, are routing business to overseas branches in countries where the rules are interpreted less restrictively, causing the loss of jobs, skills and business. It is conservatively estimated that this is causing a loss of exports from the UK worth over £50 million per annum.

In response, the ECO is pursuing six initiatives:

1) It is working with its main advisory department on this issue, the Communications-Electronics Security Group ('CESG', part of the Government Communications Headquarters, 'GCHQ') to develop a less restrictive approach, closer to the U.S. interpretation of the Cryptography Note. But ECO officials have made clear that they have no intention of adopting the U.S. concept of items that are not controlled by virtue of being 'mass market' and will not 'open the floodgates'. Broadly, it is understood that the ECO's interpretation of the Cryptography Note will remain that exemption should apply only to products intended primarily for retail to consumers and not to those intended for commercial use, even by small businesses, taking into account indicators including how widely a product is marketed, its typical customers, the volume of sales, the price, and the technical skill required for installation (in CESG's view, ordinary members of the public should be able to install the product);
2) With respect to components (i.e. 'Note 3b'), the ECO is already satisfied with being given examples of the types of product in which the component will be used without needing to know all its possible uses. In future, if a component is specifically designed for an exempted consumer-type product, then a statement of design intent may be sufficient to allow exemption of the component intended to go into it. The ECO will also consider whether to decontrol components designed for consumer-type products that are still under development. Some governments already exempt such components although, strictly, the exemption applies only to components for existing items;
3) To help exporters judge for themselves whether their products qualify for exemption (to 'self-classify'), they need the ECO's interpretation of the rules to be translated into specific, clear guidance. The ECO is developing new, expanded guidance to be published on its website and to be incorporated into its new online export licence application system, LITE (due to replace SPIRE from summer 2017). The ECO is actively seeking case studies from companies that can be used to illustrate how the rules are applied in practice;
4) Currently, if a UK exporter is unsure whether or not their goods require an export licence, the only way to obtain an official ruling is to apply for a standard individual export licence ('SIEL'). (It is advisable that the licence application should explicitly state that a ruling is being requested as otherwise there is a risk that a licence will simply be issued.) But this is time-consuming for all concerned. The ECO is planning to restart its former control rating inquiry service, possibly later this year, as soon as trained staff are available (new staff are currently in training). This will enable exporters to ask the ECO for a determination of whether a specific item is subject to control, without having to apply for a licence. The ECO is to consider including in responses by the service generic advice on how a 'No Licence Required' ruling was determined to help exporters

There are significant differences between regulators in their interpretation and application of exemptions in the Cryptography Note.

understand the rationale for the control rating, in order to be able to conduct their own classifications;

5) The ECO has initiated work with other governments in the Wassenaar Arrangement (the international export control regime that establishes the list of dual-use items used by the EU, the U.S. and most others) to revise the control specifications in Category 5 Part 2. Their aim is completely to restructure and rewrite the text, to produce a positive list of items subject to controls (in place of the current approach involving a catch-all combined with a range of exemptions). At the same time, controls on 'intrusion software' may be moved from Category 4 into Category 5. It is hoped that a revised text for this section of the list will be agreed by the end of 2016 and brought into effect next year;
6) Finally, the ECO and industry (the latter is in fact doing most of the initial work) are developing an open general export licence ('OGEL') for cryptographic items that are not eligible for exemption but are nonetheless relatively low-risk. This is addressed in the box, right.

Proposed new open general export licence ('OGEL')

The ECO is in the early stages of developing a new OGEL to cover low-risk cryptographic items, to reduce the licensing burden on exporters currently applying for SIELs or OIELs for such items. It is intended to be made available in the autumn. The key challenge is to strike the right balance between the range of the items included, on the one hand, and the range of end-users and destinations on the other.

The ECO has invited suggestions from exporters of classes and types of products which could be usefully considered for inclusion, focused on items that currently generate a high volume of standard individual export licence applications. But it does not favour categories which risk being too ill-defined and broad, such as 'items using commercial encryption'. Framing clear, effective descriptions of items to be covered is challenging and, clearly, needs to avoid including items that are already deemed not to require a licence. Initial ideas include:

- items with a government security grading up to 'Official – Sensitive';
- components for incorporation and re-export;
- products, software and technology utilising standards set out by ETSI, GSM, 3GPP etc.;
- Unified Threat Management security appliances, software and technology for commercial use;
- business transaction management software;
- general purpose storage software and hardware;
- software for data integration and analytics, and mobile and social computing;
- Commercial Secure Access Service software installed on laptops but not eligible for the 'personal use' de-controls;
- server and network hardware and software intended for non-consumer use;
- routers for commercial use in secure communications.

The industry would clearly want to have government agencies and government-controlled organisations, such as the emergency services, included as potential end-users. But doing so would be likely to lead the ECO to restrict the range of items and destinations that would be covered.

What export licences are available?

The availability of export licences for controlled cryptographic items in the UK, and in the EU more widely, is based on the combined risks of the capabilities of the item to be exported, its intended destination country and its end-user. The higher the potential level of risk, the more thorough the licensing requirement needs to be in order appropriately to assess the risk and ultimately, if there is a clear risk that the item might be misused, to refuse a licence. In the UK, there are four main types of licence available for cryptographic items.

1) *Standard individual export licence ('SIEL')*

This is the default licensing requirement, in order for the regulators to be certain of fully assessing the risks for the most sensitive items, destinations and end-users. The exporter must provide details of the item(s) and quantities to be exported, their proposed destination, their end use and end-user, certified in a signed End-User Undertaking. There is a specific requirement to state if any of the items are designed or modified to use cryptography, cryptographic techniques or cryptanalytic functions – this includes encryption, authentication and digital signatures, and both public domain and bespoke algorithms.

2) Open individual export licence (cryptographic)

OIELs (open individual export licences) permit unlimited shipments of specified items to named countries and end-user sectors, and require a signed consignee undertaking specifying the intended use of the item(s) and a business case statement providing evidence of future business. The Cryptographic OIEL has been specially designed to streamline the licensing process for lower-risk items going to lower risk destinations (N.B. China is excluded). The items may only be for use:

- by a business or academic collaborator of the licensee in their own commercial cryptographic product development activities;
- in an application designed for a civil business use;
- by a group undertaking of the licensee; or
- in medical devices.

The licence cannot be used for the export of items with cryptanalytic functions, a security grading above Unclassified, or intended for a military or government end use. Applications generally take one to two months to be processed.

3) Open individual export licence (generic dual-use)

If the Cryptographic OIEL is not applicable – for example if any intended end-users are government bodies or the destination is China – exporters may still apply for a generic

dual-use OIEL. This requires the provision of details of the items to be exported, their intended end use, destination country and the sector of the end-users (e.g. government, companies using the goods to fulfil a government contract, or non-government sectors). Depending on the number of goods and destinations covered, applications can take three to six months.

4) EU general export authorisation (EU001)
This permits unlimited shipments of most dual-use items to all end-users in Australia, Canada, Japan, New Zealand, Norway, Switzerland (including Liechtenstein) and the United States. The permitted items include all controlled cryptographic hardware, software and technology but, within 30 days of the first export, details of such items must be submitted to the ECO including:

- a general description of the items;
- all relevant encryption algorithms and key management schemes, and how they are used and implemented by the items;
- any measures taken to preclude user modification of the encryption algorithm, key management scheme or key length;
- details of pre- or post-processing of data, such as compression of plain text or packetisation of encrypted data;
- programming interfaces that can be used to gain access to the cryptographic functionality; and
- a list of any protocols to which the items adhere.

5) Open general export licence (OGEL Cryptographic Development)
This licence permits unlimited transfers of certain controlled cryptographic development software and technology provided it is only for use by the exporter, or their subsidiary or parent, in their own commercial cryptographic product development activities, or by a business or academic collaborator in such development activities pursuant to an agreement with the exporter. Software and technology related to cryptanalytic functions and specified sensitive destinations (including China) are excluded.

What else may be changing?
In recognition of the complexity and rapid evolution of these issues, the ECO will be hosting a conference in London with exporters towards the end of the year to discuss these and other questions related to export controls on cryptographic goods.

In addition to the more immediate issues outlined above, this conference may also want to consider potential developments in the EU. The European Commission is expected to publish its proposed revision to the 'Dual-Use Regulation' later this year (no more precise timing has been indicated). In its earlier public information on the proposals, the Commission stated that it was considering a number of issues relevant to controls on encryption, in particular:

- an EU general export authorisation for cryptographic items which seems likely to overlap significantly with the ECO's new OGEL outlined above;
- the possible expansion of 'catch-all' or 'end-use' controls (hitherto restricted to items that might be used in weapons of mass destruction or for military purposes in countries subject to an arms embargo) to items that might be used to violate human rights by surveillance of phone or internet use. This issue was raised by a European Parliament resolution in 2012;
- a possible requirement to apply human rights criteria not only to military items (as now) but also to dual-use items. This would particularly affect encryption and surveillance items, given the scope for their misuse by, for example, government security agencies against democratic activists. But this would not make a significant difference in the UK which already applies human rights criteria to all dual-use export licence applications.

Last but not least will be the UK's exit from the EU. This raises many questions for the future shape of the UK's export licensing and sanctions regimes. But, however the debate evolves, it is important to keep in mind that the basis of both the UK's and the EU's export controls on dual-use items is the Wassenaar Arrangement and its dual-use control list. Since there is no suggestion that the UK might end its membership of the Arrangement, it can be expected to continue to play a leading role within it and to continue to implement the same dual-use control list that forms the basis of the EU's controls. While it is possible that licensing arrangements and interpretations in the UK and the EU may diverge, as to an extent they do already, the control list will remain a common point of reference, including any changes to the controls and de-controls of cryptographic items.

Richard Tauwhare is a Senior Director at the London office of the law firm Dechert. Previously, he served in the UK Foreign and Commonwealth Office where he was head of Arms Export Control Policy until February 2014.

richard.tauwhare@dechert.com

Iran files case against the U.S.A. before the International Court of Justice

Iran has instituted proceedings against the U.S.A. in respect of alleged violations under the 1955 U.S.-Iran Treaty of Amity, Economic Relations and Consular Rights. Why and what are the likely issues and consequences of the action to be, ask Andrew Cannon, Jonathan Cross and Alex Francis.

In a press release published on 15 June 2016[1], the International Court of Justice ('ICJ') announced that Iran has instituted proceedings against the U.S.A. in respect of alleged violations under the 1955 U.S.-Iran Treaty of Amity, Economic Relations and Consular Rights (the 'Treaty').

Notably, Iran's application concerns allegations that the U.S., through measures taken under its national law, has subjected assets and interests of Iran and Iranian entities, including the Iranian Central Bank ('Bank Markazi'), to enforcement in the U.S. in violation of immunities and other principles of international law that are upheld under the Treaty.

This case is likely to put the spotlight on the legality of the wide-ranging unilateral sanctions measures that have been, and continue to be, imposed by the U.S. against Iran, notwithstanding the recent relaxation in January 2016, as well as questions of extra-territoriality and immunity under international law more generally.

The press release states that, on 14 June 2016, Iran instituted proceedings in the ICJ with regard to a dispute concerning 'violations by the Government of the United States of America of the Treaty of Amity, Economic Relations, and Consular Rights between Iran and the United States of America which was signed in Tehran on 15 August 1955…' (the 'Treaty').

As the basis for the jurisdiction of the ICJ, Iran invokes article XXI(2) of the Treaty which states: 'Any dispute between the High Contracting Parties as to the interpretation or application of the present Treaty, not satisfactorily adjusted by diplomacy, shall be submitted to the [ICJ], unless the High Contracting Parties agree to settlement by some other pacific means.'

In its application, Iran claims that the U.S. has adopted a number of legislative and executive acts that have the practical effect of subjecting the assets and interests of Iran and Iranian entities to enforcement proceedings in the U.S., including where such assets or interests 'are found to be held by separate juridical entities…that are not party to the judgment on liability in respect of which enforcement is sought', and/or 'are held by Iran or Iranian entities…and benefit from immunities from enforcement proceedings as a matter of international law, and as required by the [1955] Treaty'.

This case is likely to put the spotlight on the legality of the wide-ranging unilateral sanctions measures that have been, and continue to be, imposed by the U.S. against Iran.

Specifically, it is alleged that U.S. courts 'have repeatedly dismissed attempts by Bank Markazi to rely on the immunities to which such property is entitled' under U.S. law and the Treaty. Iran further maintains that 'the assets of Iranian financial institutions and other Iranian companies have already been seized, or are in the process of being seized and transferred, or at risk of being seized and transferred, in a number of proceedings'.

It is Iran's contention that the U.S. has breached, *inter alia*, articles III (1), III (2), IV (1), IV (2), V (1), VII (1) and X (1) of the Treaty, specifically in its alleged:

a) failure to recognise the separate juridical status (including the separate legal personality) of all Iranian companies, including Bank Markazi;
b) unfair and discriminatory treatment of such entities, and their property, impairing the legally acquired rights and interests of such entities;
c) failure to accord to such entities and their property the most constant protection and security;
d) expropriation of the property of such entities;
e) failure to accord to such entities freedom of access to the U.S. courts, including the abrogation of the immunities to which Iran and Iranian state-owned companies, and their property, are entitled under customary international law and the Treaty;
f) failure to respect the right of such entities to acquire and dispose of property;
g) application of restrictions to such entities on the making of payments and other transfers of funds to or from the U.S.A.; and
h) interference with the freedom of commerce.

The application also seeks an order and declaration from the ICJ that, *inter alia*, (i) the U.S.A. ensures that no steps be taken based on the executive, legislative and judicial acts at issue, to the extent that such acts are incompatible with the Treaty; (ii) Iran and Iranian state-owned companies are entitled to immunity from the jurisdiction of the U.S. courts, and in respect of enforcement proceedings in the U.S.A.; (iii) the U.S.A. and U.S. courts respect the juridical status (including the separate legal

Links and notes

[1] See the press release at: http://www.icj-cij.org/docket/files/164/19032.pdf

personality), and ensure freedom of access to the U.S. courts, of all Iranian companies, including state-owned companies such as Bank Markazi.

Iran also seeks reparations from the U.S.A. for these alleged violations 'in an amount to be determined at a subsequent stage of the proceedings'.

Comment

This application is an interesting development in the long and complex history of Iran-U.S. legal relations. The focus of the case appears to be the effect under international law of the U.S. sanctions regime against Iran. Although so-called 'secondary' sanctions were largely suspended following Implementation Day, the U.S. continues to impose wide-ranging 'primary' measures against Iran, applicable to U.S. persons and transactions with a U.S. nexus. It may also consider questions of the general legality of unilateral measures, including those with extra-territorial effect, as well as the approach of the U.S. courts to questions of sovereign immunity. The dispute has been brought under the 1955 Treaty which contains a provision agreeing to submit disputes to the jurisdiction of the ICJ. Accordingly, the ICJ's jurisdiction, if upheld, will be limited to matters arising under the Treaty, and in particular its 'interpretation or application'. As such, the court may not have jurisdiction over wider questions of alleged violations of international law that do not fall to be considered within the context of the Treaty.

[The application] may also reflect frustration at what Iran perceives as the slow progress since Implementation Day.

Press sources are linking the application to an April 2016 decision of the U.S. Supreme Court, which held that U.S.$2 billion in Bank Markazi funds, frozen in the U.S., could be used to satisfy default judgments in relation to Iran's involvement in foreign terrorist activities. It may also reflect frustration at what Iran perceives as the slow progress since Implementation Day, as many investors and financial institutions continue to be wary about doing business in Iran given the persistence of U.S. primary sanctions.

See Herbert Smith's public international law blog at http://hsfnotes.com/publicinternationallaw/

Andrew Cannon is a partner (Paris), Jonathan Cross is counsel (New York) and Alex Francis is an associate (Paris) at Herbert Smith Freehills.

andrew.cannon@hsf.com
jonathan.cross@hsf.com
alex.francis@hsf.com

Russia-Turkey sanctions

Presidential phone call leads to relaxation of sanctions

Following the shooting down of a Russian jet fighter by Turkish planes late last year, the Kremlin responded with sanctions. In early July, a phone conversation between the leaders of the two countries resulted in the sanctions being relaxed. Orçun Çetinkaya tells the story.

On 24 November, 2015, claiming that Turkish airspace had been violated, Turkish F-16 fighters downed a Russian Su-24 jet, causing the Russian aircraft to crash in the Bayirbucak region of northern Syria. Russia swiftly imposed a series of economic measures and sanctions against Turkey.

Those sanctions are being rolled back as a result of a phone conversation between Russia's president Vladimir Putin, and Turkey' president Recep Tayyip Erdoğan on 29 June 2016. Within two weeks of the call, charter planes carrying Russian tourists were once again landing in the tourist resort of Antalya.

Prior to the Su-24 incident, Turkey had been one of the most popular destinations for Russian holidaymakers, and the cost of sanctions to the sector has been estimated as being in the region of $10bn.

Other parts of the economy hard hit by the sanctions include agriculture (Russia is a major importer of Turkish agricultural products, fruits and goods), and construction – in recent decades, Turkish companies have won large contracts on projects from dams to major shopping malls and road-building. Many of these projects ground to a halt as a result of the sanctions.

The sanctions had comprised a number of special economic and administrative measures against the Republic of Turkey, and were imposed by Decree No. 583, signed by the President of the Russian Federation ('the RF President') on 28 November 2015, in connection with the events that took place near the border between Syria and Turkey and detailed in the decisions of the Government of the Russian Federation ('the RF Government').

The decree came into force on the date of its signing, and provided, *inter alia*:

- A ban or restriction on foreign trade operations related to importing certain goods originating from Turkey into Russian territory;
- A ban or restriction on organisations under the jurisdiction of Turkey as well as legal entities controlled by Turkish nationals or organisations under the jurisdiction of Turkey, performing (providing) certain types of works (services) in Russian territory;
- A ban for employers and customers of works (services) not included in the list approved by the RF Government on engaging Turkish nationals who are not in employment and (or) civil-legal relationships with such employers, customers of works (services) as of 31 December 2015, in employment relations, performance of works and provision of services, effective from 1 January 2016;
- A suspension from 1 January 2016 of the agreement between the RF Government and the government of Turkey for the terms and conditions of mutual trips of citizens of the Russian Federation and nationals of Turkey dated 12 May 2010, in terms of travels by Turkish nationals to Russia without visas, with certain exceptions.

Decree No. 583 also required tour operators and travel agencies to abstain from selling tours to Turkey to Russian citizens.

Connected to this, the RF Government was instructed to take measures:

- to introduce a ban on charter flights between Russia and Turkey;
- to strengthen control over Turkish road carriers in Russian territory to ensure safety;
- to strengthen control in Russian waters and seaports in the Azov-Black Sea basin, including in order to prevent illegal staying and movement of marine and other vessels over there.

Decree No. 583 also required tour operators and travel agencies to abstain from selling tours to Turkey to Russian citizens.

The bans and restrictions under Decree No. 583 and the RF Government's related decisions affected:

- Wholesale suppliers and buyers (importers) of (newly) banned goods;
- Organisations under Turkey's jurisdiction (i.e. established and existing under Turkish laws), as well as legal entities controlled by Turkish citizens or organisations under Turkey's jurisdiction, branches and representative offices of such organisations in Russia, that perform/provide the works/services which are banned in Russian territory;
- Employers and customers of works (services) in Russia that engage Turkish citizens starting from 1 January 2016, irrespective of their nationality, except for those specifically exempted from RF Government decisions;
- Travel agents, tour operators and other parties engaging in charter flights between Russia and Turkey,

as well as those who organise Turkish trips and tours for Russian citizens;
- Airline companies providing charter flights between Turkey and Russia;
- Automotive carriers providing bilateral carriages between Turkey and Russia;
- Turkish nationals travelling on business and other trips to Russia for up to 30 days. (An exception applies for those with a temporary residence permit or a residence permit for the territory of Russia, as well as for those involved in Turkish diplomatic and consular missions in the territory of Russia, provided they have valid official and special passports, together with their families.)

On 30 June, the Russian President issued Decree No. 314 to substantially, though not entirely, lift the sanctions. The decree

- provides for the resumption of charter flights between Russia and Turkey;
- allows Russian travel agencies to sell tours to Turkey; and
- instructs the RF Government to hold negotiations with the government of Turkey on the improvement of foreign economic relations, which may result in gradual repeal of the other foreign trade measures currently imposed.

On 30 June, the Russian President issued Decree No. 314 to substantially, though not entirely, lift the sanctions.

It is intended that the decree will be implemented through the necessary and relevant resolutions of the RF Government.

On 13 July, the Turkish government announced: 'Upon the invitation of the Russian Federation authorities and with the purpose of discussing the cooperation and relations in the field of tourism between Turkey and Russia, a Turkish delegation will hold talks with Russian counterparts in Moscow on 14 July.

'The Turkish delegation will be headed by the Ministry of Foreign Affairs and consist of the authorities from the Ministry of Culture and Tourism, the Ministry of Transport, Maritime and Communications and the Ministry of Interior, as well as the representatives of the private sector.'

As at time of writing, the outcome of those discussions is yet to be announced.

Orçun Çetinkaya is a partner at Moroğlu Arseven in Istanbul. He regularly supports both local and foreign clients in cross-border matters.

ocetinkaya@morogluarseven.com

THE WORLDECR EXPORT CONTROLS AND SANCTIONS FORUM 2016

LONDON

Official sponsors

Graf von Westphalen

BRAUMILLER LAW GROUP, PLLC
INTERNATIONAL TRADE LAW

Hogan Lovells

Dechert LLP

Amber Road
POWERING GLOBAL TRADE

Official evening reception sponsor

Debevoise & Plimpton

13-14 OCTOBER, 8 FENCHURCH PLACE, LONDON EC3

Welcome

Tom Blass, Editor, WorldECR

October 13 and 14 sees what has now become a regular fixture in the compliance calendar – the *WorldECR* Export Controls and Sanctions Forum in London – the fourth thus far.

As in previous years, our speakers will be honing in on critical and timely issues in trade compliance from a uniquely cosmopolitan stance. We'll be welcoming presenters from China, Singapore, South Africa, Canada, the United States and the European Union – sharing knowledge of a diverse range of sectors and viewpoints, amongst them:

- Airbus's post-JCPOA contract to meet the Government of Iran's aviation needs
- Oil service company Weatherford's response to sectoral sanctions against Russia
- Recent developments in and challenges for the multilateral export control regimes
- Industry's role in capacity-building for nations still developing export controls
- The emergence of strategic trade controls in SE Asia
- The challenge of making intra-company transfers with minimum fuss and maximum compliant efficiency
- The future of U.S. sanctions and exports controls in the 'post-Obama' world

As ever, we'll be encouraging robust discussion and debate both within the conference room and during break-outs. Regular attendees of our Forum know that we take great lengths to create a collegiate, professional but also highly enjoyable event, hallmarked by our unique focus on, and interest in, the convergence of foreign policy, law and business: the world of sanctions and export controls.

As in previous years, there will be a drinks reception at the end of Day One, this year kindly sponsored by international law firm Debevoise & Plimpton, and the option to enjoy a relaxed and informal dinner for speakers, panellists and delegates. It is optional and there is an additional charge, but it always proves a fun end to the first day and is a great opportunity to share ideas and make friends and acquaintances with others in the world of trade compliance.

Key dates and offers

Please allow me to draw your attention to the following promotions:

- If you register by 20 September you can save £200
- Additional delegates from the same organisation can save an additional £100.

Tom Blass
Editor, WorldECR

Contents of this programme

Josh Fitzhugh – Why it's right to put export control compliance at the heart of the business

Over the past five years the UK-managed portion of BAE Systems has revolutionised the way it approaches export control compliance. It has transformed from a small, decentralised group of ad hoc practitioners with little in the way of formal procedure and process into a corporate function with a defined mission, a robust procedural framework and a world-class functional capability.

The revolution has been a successful one. The company embraces a culture of compliance, and over the past five years has adopted a new Export Control Policy and Export Control Procedures and new ways of delivering and assuring compliance. Businesses and functions within the company have embedded the new requirements into their day-to-day activities.

In this presentation, Josh Fitzhugh, Group Head of Export Controls, will talk delegates through this compliance revolution, the challenges, and also its benefits, which have included better information on jurisdiction, classification and licensing; increased communication with third parties and suppliers; and significant improvements in overall compliance. As the company strives for excellence in customer focus, financial performance, programme execution and responsible behaviour, it knows effective compliance is a key element to realising these goals, and indeed to its ability to operate in the global marketplace.

Pierre Cardin – Wings over Tehran

In late January this year, shortly after Implementation Day, and taking full advantage of the post-JCPOA 'détente', Airbus announced that it had signed a preliminary deal with Iran Air that will see the airline take delivery of 118 aircraft – with associated training and support services. The company also signed a civil aviation co-operation agreement with the Iranian Minister of Roads and Urban Development.

Many companies remain wary of business with Iran, despite the dismantling of U.S. secondary sanctions and some EU restrictive measures – but Airbus has proven itself ready to meet the country's urgent aviation needs.

In his presentation, Pierre Cardin, Airbus Group Export Compliance Officer, talks through the obstacles and how they were surmounted.

Roger Matthews – BREXIT and its possible implications

The result of the United Kingdom's referendum on its European Union membership has opened a veritable Pandora's Box about the UK's future trading relationships and more.

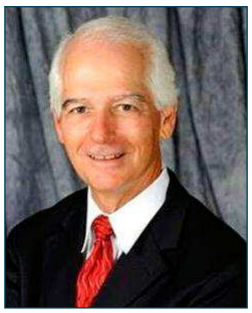
Will 'splitting the pack' have diluted the EU's effectiveness as a foreign policy player? And will the UK begin to consolidate its own unilateral approach to foreign policy and sanctions issues? How will intra-EU exports of dual-use goods be affected by BREXIT? Will long-established procedures, well understood by industry, require wholesale revision? And what will BREXIT mean for trading partners with the UK from beyond the EU, such as the United States, Canada and Asia?

So far, clear answers to such questions have yet to emerge (indeed, it may be months before they do). But in this presentation Roger Matthews, senior lawyer at Dechert LLP, explores how business should be taking stock of Britain's momentous move out of Europe.

Ajay Kuntamukkala and Lourdes Catrain – Intra-company transfers: Straightforward? Not always. But they needn't be painful

Transferring controlled goods, services, and data and information between a company's international locations should be straightforward – but as many compliance officers know all too well, it can prove to be a headache.

This presentation by Ajay Kuntamukkala and Lourdes Catrain of the Washington, DC and Brussels offices of international law firm Hogan Lovells is a step-by-step account of best practice in making intra-company transfers and describes how the process can be rendered less painful. The discussion will cover U.S. and EU requirements that apply to intra-company transfers, available exceptions and general licences, and practical tips for structuring compliance programmes.



Bruce Leeds – Taking stock of U.S. Export Control Reform, present and future

The U.S. Export Control Reform Initiative – launched back in 2009 so as to more accurately address security threats while ensuring U.S. competitiveness – is part way through the second of its three phases, with many of the definitions and regulations that have distinguished and differentiated the two regimes of the Export Administration Regulations ('EAR') and the International Traffic in Arms Regulations ('ITAR') now reconciled, and numerous items moved away from the U.S. Military List to the Commerce List.

Compliance professionals affected by ECR (particularly those working in ITAR-focused industries) have largely adjusted to the implications of the changes. But are there more to come?

As the Obama presidency nears completion, how far is the Initiative from doing the same? How is a change of Administration in the U.S. likely to affect the Initiative? And should European businesses and the Europe-based subs of U.S. companies expect and prepare for further evolution or revolution?

Bruce Leeds, of counsel at Braumiller Law Group, outlines his thoughts on the future of ECR and the impact for all export compliance practitioners.

Alex Parker and Konstantin Bureiko – Update on key EU sanctions developments

Since taking the helm as High Representative for Foreign Affairs and Security, Federica Mogherini has steered the European Union's increasingly significant role as a player in international affairs. Much of that, of course, has been exercised through the prism of EU restrictive measures.

2015/2016 has seen the ratcheting up of pressure against Russia and North Korea and the so-called Islamic State, and the suspension or relaxation of measures against Iran and Belarus. Each impacts on the scope of a company's regional operations – indeed, the shifting topography of EU sanctions has been keeping business very much on its toes.

In this presentation, Alex Parker and Konstantin Bureiko of law firm Debevoise & Plimpton scope out the measures taken by the EU to assert its foreign policy position, the overlap with actions taken by the U.S. Department of State, how they've been applied in practice, appropriate responses, and where policy might be headed in 2017.

Julie Cooper – Weathering the storm: How an oil service company navigated new territory in Russia

Between March and September 2015, the European Union and the United States imposed sanctions against Russia in response to what both saw as the Kremlin's destabilisation of Ukraine and annexation of Crimea. Amongst the measures were included a requirement for the prior authorisation of energy-related equipment and technology – with a presumption of denial for some kinds of deepwater and Arctic projects.

As an international oil and gas service company, Weatherford belongs to an industry that finds itself particularly affected by the sanctions and restrictive measures imposed on Russia by the United States and European Union in the wake of Moscow's annexation of Crimea. Indeed, the new 'sectoral' restrictions – imposing restrictions on the export of certain classes of goods and services – marked a new approach to trade control when imposed on both sides of the Atlantic.

Julie Cooper, Weatherford's Regional Trade Compliance Manager for Europe, the Caspian and Russia, describes how her company adjusted to a chillier climate.

Panel Discussion – Staying compliant through multiple jurisdictional layers: is it possible?

The challenge for a global business is to stay compliant in all the jurisdictions in which it operates, whether that's as a distributor, manufacturer or service provider. But how is this done? And how are inconsistencies managed and resolved?

Each of our panellists has many years' experience navigating the practical, legal and management issues that multinational business encounters. In this session, they will share thoughts and invite insight and discussion from delegates as they look for answers to key questions, such as:

- How different are the perspectives of parent and subsidiary companies, when each is subject to the laws of a different country?
- How much autonomy and responsibility for compliance decisions is it appropriate to allocate to different divisions of a company's operations?
- How should jurisdictional requirements be prioritised?
- Is a single Internal Compliance Plan appropriate in the age of global business or a false comfort that ignores the reality of complex and conflicting regulatory frameworks and policy imperatives?

Moderating this session will be Jay Nash, Managing Director of Strategy & Development at SECURUS trade consultants. Jay and his SECURUS colleagues have experience of navigating export control regimes in more than 50 countries around the globe.

Joining Jay on the panel are:

- Carmen Fellows, Senior Director, Global Trade Compliance, Finmeccanica North America and DRS Technologies, Inc
- Burim Ceni, Senior Manager Trade Compliance, RUAG Aviation
- Bernadette Peers, Compliance Manager, Strategic Shipping Company Ltd, and Chair, Export Group for Aerospace, Defence & Dual-Use
- Allison Porcella, Head of Trade Compliance, SR Technics

Lothar Harings and Marian Niestedt – A German perspective on EU trade controls: policy and practice

Germany is Europe's largest exporter of hi-tech goods and plant machinery – and traditionally a major business partner of Iran. Its main regulatory authority, BAFA, the entity which handles licence applications, has developed a reputation for interpreting EU sanctions and export controls with thoroughness and rigour.

This is all the more relevant since approximately 60% of all licence applications within the EU are handled by BAFA.

Indeed, given Germany's pre-eminent role in the EU economy – and its broader political influence both regionally and internationally – the importance of understanding German export control policy and procedure cannot be underestimated.

In their presentation, Lothar Harings and Marian Niestedt, partners at law firm GvW Graf von Westphalen, describe BAFA's approach and outline the five must-knows for exporters from Germany and their partners.

Richard Tauwhare – EU export controls on cryptography, software and The Cloud

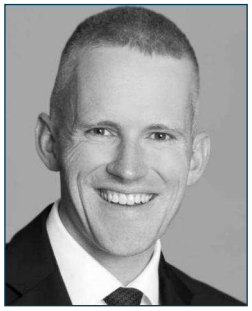
An important session not only for providers of Cloud services – but exporters of cryptography and users of 'the Cloud' (and these days that includes most of us!).

Richard Tauwhare, senior Director of Export Controls and Sanctions at the London office of Dechert LLP (and former head of the Arms Export Policy Department at the Foreign and Commonwealth Office) describes the current state of EU export controls on encryption products, 'the Cloud' and related technology.

Richard will discuss:

- The areas subject to export controls – cryptographic hardware, software, and technology
- What is exempt and how can you tell
- Key differences between EU and U.S. controls
- Which export licences are available and when to use them

This is a must-attend session for all users of encryption products and of Cloud services – and all the more critical coming at this time of potential change in EU export controls, generally.



Burim Ceni and Hugo Munthe-Kaas – In Europe but not the EU: the experience of Norway and Switzerland

Not surprisingly, given that 28 states are (currently) members, the Europe Union has become as good as synonymous with the notion of 'Europe' as a whole: and thus the continent is bound by an obligation to adhere to the same Brussels-driven directives and regulations concerning export controls and restrictive measures.

But there are important exceptions. In those countries that have chosen not to accede to the European Union –Norway, Switzerland, Iceland – as well as the EU candidate countries of the Balkans and Eastern Europe, export control policy and practice tend to adhere closely to the contours of EU regulation, though there can be significant if subtle differences and points of departure.

Hugo Munthe-Kaas of Norwegian law firm Thommessen, and Burim Ceni, Senior Manager Trade Compliance, RUAG Aviation, Switzerland, share and compare their experiences, and invite delegates' questions on Europe outside of the European Union.

A 'must-attend' session for any compliance person currently working in a country that may leave the EU in the foreseeable future!

Virusha Subban – Introducing South African export controls

The Republic of South Africa is the only sub-Saharan country to have signed the Wassenaar Arrangement. It possesses the most sophisticated export control regulatory framework on the continent.

Key legislation regulating exports from South Africa includes the Non-Proliferation of Weapons of Mass Destruction Act and the National Conventional Arms Control Act. International trade in South Africa comes within the ambit of a number of agencies, including the Department of Minerals and Energy, the Department of Trade and Industry and the Department of Defence. Each has a role to play in the administration and authorisation of the export of controlled goods, as Virusha Subban of the law firm Bowman Gilfillan describes.

Virusha will also describe the sectors typically impacted by South African export controls, and the practical issues they encounter in dealing with the relevant agencies.

Johnny Xie – China's export control system

China is the world's second-largest economy, and recently surpassed the United States as the world's largest trading nation – with annual trade in goods valued at around $4 trillion. While not a member of the Wassenaar Arrangement, the MTCR or the Australia Group, its control lists and legislation are sophisticated and extensive – if not always easy to navigate.

Johnny Xie, general manager of Tradewin – whose previous experience includes working both for Chinese Customs and U.S. corporations and consultancies – is among a handful of professionals able to give a lucid explanation of Chinese export controls in law and practice. In addition to describing the relevant legal framework and respective role of ministries, Johnny will walk delegates through the licences available to exporters, how to apply and whom to apply to, and the distinctive features of China's control lists.

This is a must-attend session for anyone doing business in China.

George Tan – South East Asian export controls come of age: update on Thailand, Philippines and beyond

For years, export control regimes in much of SE Asia (including Thailand, the Philippines and elsewhere) were under discussion, but largely remarkable by their absence. But Thailand and Philippines have both introduced new laws which, once in play, will change that – creating new compliance obligations not only for domestic companies, but for foreign parent companies and investors alike.

George Tan, director of Global Trade Security Consulting in Singapore, one of only a very few people to possess a holistic appreciation of Asian strategic trade controls, assesses the state of play.

Ryan Lynch Cathie – All change for India

India's recent accession to the Missile Technology Control Regime ('MTCR') – and speculation that it may yet join the Nuclear Suppliers Group ('NSG') – has further emphasised the country's commitment to international export control standards. Less well-known is the increasing interest amongst Indian companies in sharing, disseminating and adopting best practice.

At the heart of the country's export control system is its list of 'SCOMET' (Special Chemicals, Organisms, Materials, Equipment and Technologies) items, which in the past year has seen noteworthy revisions.

In his presentation, Ryan Lynch Cathie, Managing Director of Products and Innovation at Securus Strategic Trade Solutions, outlines these and other important changes to the Indian export control regime over the past year.

Lourdes Catrain and Stephen Propst – Fear and Trembling: the enforcement session

Reporting of enforcement by regulators in export control and sanctions matters gravitates around hard-hitting penalties and sometimes imprisonment. But beyond the headlines, there are many important questions to be answered:

- What are the subtler trends beneath the headlines?
- About whom and what kind of activities are the regulators concerned and why?
- Are million-dollar fines the only tools they have at their disposal?
- And how do companies handle enforcement actions involving multiple jurisdictions and multiple agencies?

This session, from Hogan Lovells' Stephen Propst and Lourdes Catrain, shines a light on the hows and whys of enforcement in the U.S. and EU.

Cyndee Todgham Cherniak – Hotting up! Export controls and sanctions in Trudeau's Canada

Canada is generally considered to be passive in terms of trade controls in comparison with the United States. Well, things are getting more dynamic.

Cyndee Todgham Cherniak, of Toronto-based specialist trade law firm LexSage, outlines recent key developments in Canadian trade controls and regulation that all export compliance managers should be aware of, including:

- Changes to Canada's economic sanctions against Iran and Russia
- Changes to Canada's export controls against Belarus
- Recent cases under the Special Economic Measures Act
- Recent cases under the Export and Import Permits Act
- Update on developments under the Trudeau government

Tom Keatinge – Banks and trade finance: managing an increasingly complex relationship

Due diligence pressures on banks get ever greater as regulatory expectations placed on the financial sector rise. At best, this rising burden leads to greater disclosure demands on their clients and account-holders; at worst, it leads to the termination of business relationships. Why is this?

In this presentation, Tom Keatinge, formerly of JP Morgan and now Director Of The Centre For Financial Crime And Security Studies At The Royal United Services Institute ('RUSI'), will provide an insight into the compliance approaches taken by banks to trade finance and propose means by which industry can facilitate relationships with banks and mitigate the risk of business disruption.

Alex Parker and Konstantin Bureiko – Investigations: Responses, process and challenges

An investigation is something a company usually wants to avoid – not least because of the potential collateral fall-out such as loss of company morale and reputational damage.

But if well conducted, the benefits to a corporation can far outweigh any such damage, as this session from Alex Parker and Konstantin Bureiko of international law firm Debevoise & Plimpton on sanctions-related investigations in Europe will demonstrate.

Amongst other areas covered, Alex and Konstantin will discuss how to respond to an enforcement action or a whistle-blowing event, the environment for self-reporting, what steps to take at the start of an investigation, and issues of data-sharing with non-EU regulators.

THE WORLDECR EXPORT CONTROLS & SANCTIONS FORUM

13-14 October 2016, 8 Fenchurch Place, London EC3

REGISTRATION FORM

Please register the following delegate(s) for The WorldECR Export Controls and Sanctions Forum 2016

Delegate 1	Delegate 2
NAME	NAME
POSITION	POSITION
❑ Conference only ❑ Conference + dinner (please tick)	❑ Conference only ❑ Conference + dinner (please tick)
Organisation	
Address	**Delegate 3**
Address	NAME
City	POSITION
Post/Zipcode	❑ Conference only ❑ Conference + dinner (please tick)
Country	**Delegate 4**
Telephone	NAME
Email	POSITION
	❑ Conference only ❑ Conference + dinner (please tick)

FEE PER 1ST DELEGATE (INCLUDES VAT @ 20%)

REGISTER & PAY	BY 20 SEPTEMBER 2016	AFTER 20 SEPTEMBER 2016
CONFERENCE	£1095 + VAT = £1314	£1295 + VAT =£1554
CONFERENCE + DINNER	£1145 + VAT =£1374	£1345 + VAT = £1614

FEE PER ADDITIONAL DELEGATE (INCLUDES VAT @ 20%)

REGISTER & PAY	BY 20 SEPTEMBER 2016	AFTER 20 SEPTEMBER 2016
CONFERENCE	£995 + VAT = £1194	£1195 + VAT =£1434
CONFERENCE + DINNER	£1045 + VAT = £1254	£1245 + VAT = £1494

HOW TO PAY*

1) ☐ I will pay by card on line: please go to www.worldecr.com/conference-payment

2) ☐ Please invoice me.
Please email your completed registration form to mark.cusick@worldecr.com

3) ☐ I am paying by cheque

I have enclosed a cheque made payable to D.C. Houghton Ltd for £_____

Please send your completed registration form with cheque to: D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road, London N1 7GU, England

Signed _____ **Date** _____

***PAYMENT OPTIONS FOR NON-UK DELEGATES**
Non-UK-based delegates may be able to avoid paying VAT. For further details – or if you prefer to pay in a different currency – please email mark.cusick@worldecr.com

Terms and conditions
Please note, by registering for this event you accept the terms and conditions below.

Registration Fee
Your fee includes the attendance at both days of the conference; morning, mid-morning and afternoon coffee and pastries, and lunch on both days; drinks reception on day 1; programme materials.

Registration policy
Delegates may not 'share' a registration without the organiser's authorisation.

Payment policy
Payment must be received in full by the conference date. 'Additional delegate' prices are only available to delegates from the same organisation as the original full-fee delegate.

Cancellations and Refunds
You must notify the conference organiser 48 hours before the conference if you wish to change the delegate.

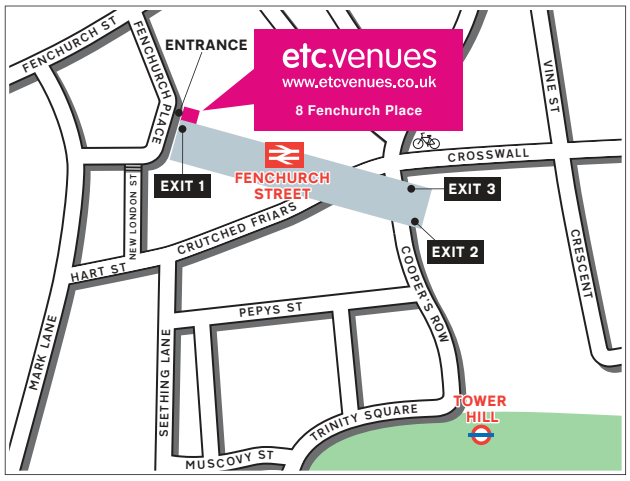
If you wish to cancel your registration, you can do so incurring the following charges:
Cancellation more than 28 days before the event – full refund less 33% admin fee.
Cancellation between 27 and 6 days before the event – full refund less 50% admin fee.
Cancellation between 5 days before and the day of the event – no refund.

Change of venue
The organisers reserve the right to change the venue should attendance numbers so demand.

Change of speaker and presentation
The organisers reserve the right to change speakers and/or presentations.

For all payment enquiries, contact WorldECR's publisher, Mark Cusick at mark.cusick@worldecr.com

How to find etc.venues Fenchurch Place



8 Fenchurch Place is located through a large white doorway right next door to Fenchurch Street mainline station – also a short walk from Tower Hill underground and DLR stations. It's also well within a 15 minute walk of Aldgate, Bank and Monument Stations.

By train
8 Fenchurch Place is situated right next door to Fenchurch Street station. Exit the station via Exit 1 which can be found at the end of Platforms 1-4. When using Exit 1 simply turn right out of the station, the main entrance to etc.venues 8 Fenchurch St is through the large white arch.

If you exit Fenchurch St via Exits 2 & 3, you will need to turn right upon exiting the stations and onto *Coopers Row**, from here follow the directions as outlined below for the exiting the Undeground.

By Underground
District or Circle Lines to Tower Hill Station. Tower Hill is approximately 5 minutes walk.

From either Eastbound or Westbound platforms, follow the Way Out signs saying Fenchurch Street and Tower Gateway DLR. Go up the steps and into the station ticket area. Turn right out of the station and onto *Coopers Row**.

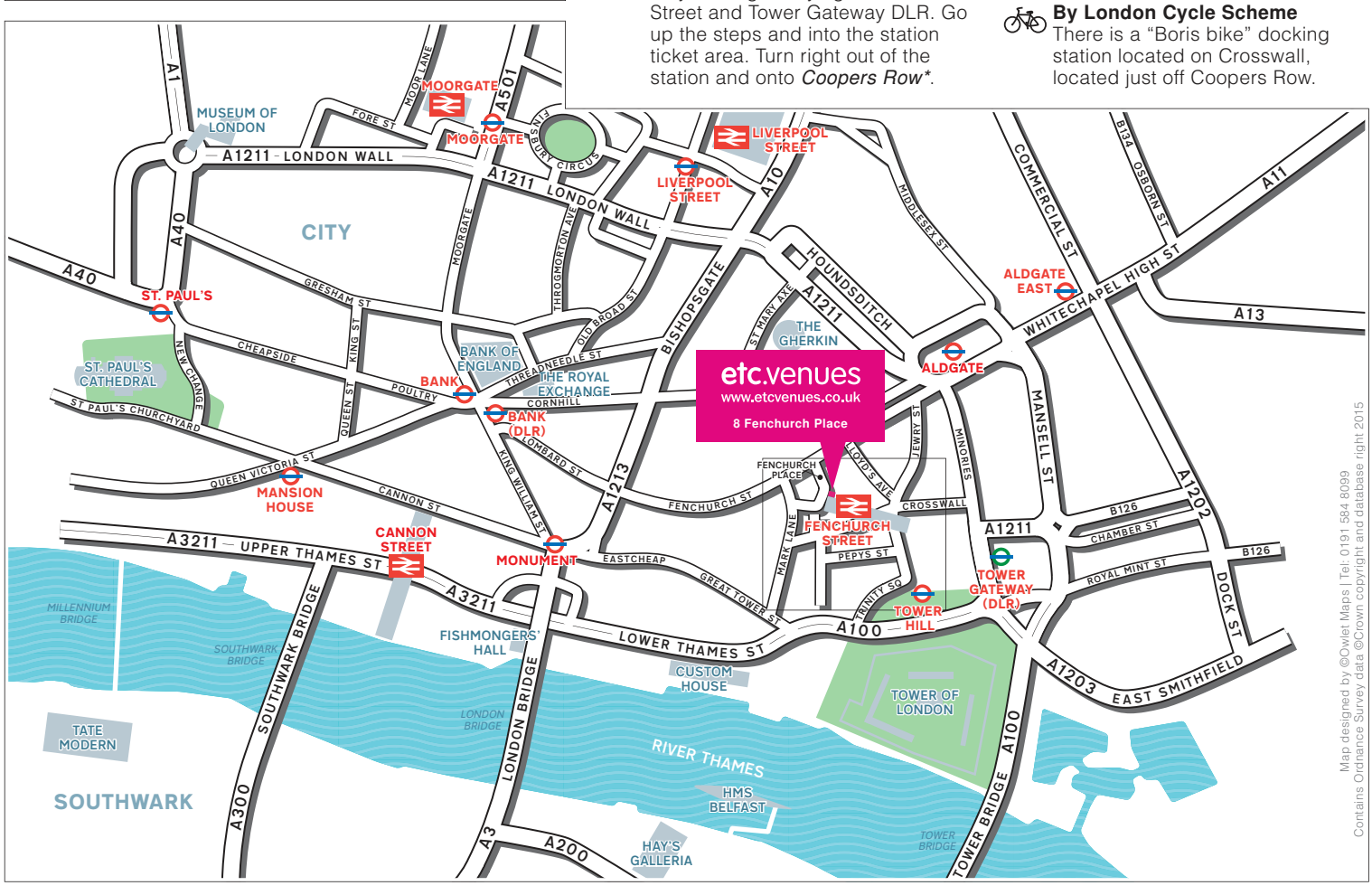
Follow Coopers Row for 250 metres (you'll see a large stone railway bridge ahead of you) and at the end of the road, just after the bridge, turn left onto Crutched Friars. Carry on down Crutched Friars for 250 metres and then turn right into New London Street. Walk along this street for 50 metres and up some steps. 8 Fenchurch Place is located to the left of the main Fenchurch Street station entrance.

By DLR
Tower Gateway Station is approximately 7 minutes walk

At the station exit, cross over the Minories and follow signs to Tower Hill underground station (100 metres away). Just before the underground station entrance, turn left down the steps. At the bottom of the steps, turn right, up a slope with steps at the end. At the top of the steps, turn right and walk towards the underground station exit (25 metres up on the right hand side). Follow the directions from * above.

By bus
8 Fenchurch Place is served by many bus routes including the 35, 47, 48 and 149.

By London Cycle Scheme
There is a "Boris bike" docking station located on Crosswall, located just off Coopers Row.



etc.venues
www.etcvenues.co.uk

8 Fenchurch Place, London EC3M 4PB

Tel: 020 3735 2700 Fax: 020 7793 4201
Email: fenchurch@etcvenues.co.uk
Sat nav: 51.511805, -0.079185

HOTEL CHOICES

The area around Fenchurch Street is well served by hotels.

We have negotiated a special reduced rate with the 5-star **Grange Tower Bridge hotel,** 45 Prescot Street, London, E1 8GP. This hotel is just a few minutes' walk from the venue.

To take advantage of the special rate when booking, contact the hotel directly by phone on **+44 (0) 20 7959 5000** or email **reservations@grangehotels.com** and quoting the special booking code **121016BR.**

Alternative hotels nearby include: Guoman Tower Hotel; Doubletree by Hilton; Apex City of London Hotel; and The Chamberlain Hotel.

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Ed Krauland and Peter Jeydel, Steptoe & Johnson LLP
www.steptoe.com

Kay Georgi, Regan Alberda and Julia Diaz, Arent Fox
www.arentfox.com

Richard Tauwhare, Dechert
www.dechert.com

Andrew Cannon, Jonathan Cross and Alex Francis, Herbert Smith Freehills
www.hsf.com

Orçun Çetinkaya, Moroğlu Arseven
www.morogluarseven.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 [0052]

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 52. JULY/AUGUST 2016
www.WorldECR.com