

WorldECR

FedEx sues Commerce, saying: ‘We’re not a law enforcement agency’	2
UK seeks stay on Saudi arms block	6
Russia facing more US sanctions	14
New US sanctions aim to cripple Cuba’s economy	19
European Council issues negotiating mandate for recast Dual-Use Regulation	23
China already implementing new export control law in response to Huawei restrictions	26
Thailand to start enforcement of export controls in 2020	28
Utilising identity access management solutions to safeguard sensitive data	30



FedEx sues Commerce, saying: ‘We’re not a law enforcement agency’

On 24 June, international freight carrier FedEx announced that it had filed a suit in the US District Court in the District of Columbia against the US Department of Commerce ‘seeking to enjoin the US Department of Commerce from enforcing prohibitions contained in the Export Administration Regulations (‘EAR’) against FedEx.’

The company said: ‘FedEx believes that the EAR violate common carriers’ rights to due process under the Fifth Amendment of the US Constitution as they unreasonably hold common carriers strictly liable for shipments that may violate the EAR without requiring evidence that the carriers had knowledge of any violations. This puts an impossible burden on a common carrier such as FedEx to know the origin and technological make-up of contents of all the shipments it handles and whether they comply with the EAR.’

It said: ‘We have invested heavily in our internal export control compliance program. However, we believe that the EAR, as currently constructed and implemented, place an unreasonable burden on FedEx to police the millions of shipments that transit our network every day. FedEx is a transportation company, not a law enforcement agency.’

‘Even if it could inspect every shipment, the complexity of the EAR would render such a potentially privacy-infringing program ineffective,’ the suit says, arguing that ‘Common carriers, as transporters for the public, cannot reasonably be expected to police the contents and



FedEx believes that the EAR ‘place an unreasonable burden on FedEx to police the millions of shipments that transit our network every day.’

ultimate destinations of the millions of daily shipments to ensure compliance with the EAR. Without a safe harbor, the EAR give FedEx two options: continue to operate under threat of imminent enforcement actions, or cease operations that may conceivably lead to enforcement and face possible legal consequences from customers and foreign governments.

‘The Due Process Clause of the Fifth Amendment to the US Constitution was enacted to prevent such oppression and deprivations of liberty. Accordingly, FedEx brings this action for declaratory and injunctive relief to secure its constitutional due process and other rights which are imminently threatened by Defendants’ enforcement of provisions of § 736 the EAR.

‘Further, the regulatory regime imposed by the EAR is such a substantial burden that it deprives FedEx of substantive due process under the Fifth Amendment. Thus, this Court should review, declare unlawful, and permanently enjoin Defendants’ unconstitutional actions. Further, in

implementing this regulatory regime, Defendants have exceeded their statutory grant of authority under the ECRA [Export Control Reform Act], and Defendants’ actions must be enjoined.’

Huawei link

Media reports have linked the suit with delivery problems encountered involving Huawei goods. The suit, however, does not make explicit mention of the Chinese telecoms company (recently added to the EAR Entity List).

Ryan Fayhee, partner at law firm Hughes Hubbard, told *WorldECR* that it was certainly true that the Huawei Entity listing presents ‘unusual’ challenges for FedEx and other common carriers, both due to the size of Huawei’s business and the complexity of its supply chain.

‘It continues to be a rare event that such a large organisation would be placed on the Entity List and many companies have confronted and struggled to manage the deep impact and disruption of the listing,’ he said.

In addition, he observed, while the Entity listing significantly limits opportunities to continue to supply goods, it does allow some business so long as the sale of components fall below the *de minimis* US content threshold.

‘This is a key distinguishing feature of the Entity listing in comparison to a designation on OFAC’s SDN list. It does, however, have a thick layer of complexity. It is straightforward for a company to simply screen against the SDN list and restrict all exports and services to any prohibited party. In contrast, the Entity listing would essentially require FedEx to understand whether the components inside a box are subject to the EAR based on content, a clear impossibility given the volume of shipments. And so, they are indeed left with the option of either restricting all shipments to Huawei entities, or carefully scrutinise each and every shipment anywhere in the world to ensure that the company is not aiding and abetting an export violation.’

Nonetheless, he said, the suit may prove to be an ‘uphill battle – given the deference to the executive branch in national security concerns and the somewhat novel due process theory, particularly where no enforcement action has been initiated.

‘In any event,’ he added, ‘the lawsuit seems clearly designed to relieve pressure on China-based FedEx employees who would be put in the position of enforcing a restriction that the Chinese government has protested vehemently.’

Commerce implements President's Huawei 'directive'

Speaking at the Bureau of Industry and Security's annual update in Washington, DC, on 9 July, US Commerce Secretary Wilbur Ross provided some clarity to companies curious to know the consequences of President Trump's apparent intervention in the Huawei affair, made during the G20 Summit.

The Chinese telecoms firm was placed on the Commerce Department's Entity List on 16 May. Shortly after, amidst not insignificant consternation from US technology companies concerned at the impact of the listing on their supply chains, Commerce issued a temporary general licence, intended, as Ross explained, to allow customers 'time to arrange new suppliers, and for Commerce to determine the appropriate long-term measures for American and foreign telecom providers currently relying on Huawei for critical services.'

In late June, President Trump announced that, following talks with his Chinese counterpart, US companies would be allowed to resume business with Huawei. Sanctions and export control lawyers, however, urged caution – pending confirmation of the situation by the Commerce Department.

In his 9 July address, Secretary Ross said: 'To implement the President's G-20 Summit directive two weeks ago, Commerce will issue licenses where there is no threat to U.S. national security. Within those confines we will try to make sure that we don't just transfer revenue from the U.S. to foreign firms. Huawei itself remains on the



Sanctions and export control lawyers have urged caution when considering resuming business with Huawei.

Entity List, and the announcement does not change the scope of items requiring licenses from the Commerce Department, nor the presumption of denial.'

As at writing time, the compliance community – and business generally – awaits further details and continues, as one lawyer put it, 'to be doing a heck of a lot of *de minimis* calculations on behalf of clients.'

Aside from the practicalities of compliance, concerns have been raised that the administration intends to use Huawei as a pawn in a larger trade war with China.

'This is muddling two different things. You can't say, "We must sever links with Huawei because it's spying on Americans," and then the next day say that a deal has been done, and business is resumed. It's either a national security issue or it isn't,' complained one lawyer.

What is also clear is that the move to place Huawei on the Entity List was met with considerable push-back from US industry: Bloomberg reported that it had seen a letter written by the Semiconductor Industry Association ('SIA'), that said, 'Overly broad restrictions that not only constrain the

ability of U.S. semiconductor companies to conduct business around the world, but also casts U.S. companies as risky and undependable, puts at risk the success of this industry, which in turn impacts our national security.'

Following Trump's apparent softening of the US stance in Osaka, SIA issued the following statement: 'The progress made today by President Trump and President Xi in Osaka is good news for the semiconductor industry, the overall tech sector, and the world's two largest economies. We are encouraged the talks are restarting and additional tariffs are on hold and we look forward to getting more detail on the president's remarks on Huawei.'

Unreliable Entity threat

As the Huawei dispute gathered pace, Chinese media reported that the country is to roll out measures in response to the listing of Huawei which will include restrictions on exports of technologies and rare earths necessary for the production of high-tech products.

A Chinese trade expert told *WorldECR* that China has a number of potential

retaliatory measures available to it, some of which he described as 'tit for tat', while others are best described as long-term, strategic countermeasures.

China's Ministry of Commerce ('MOFCOM') recently published an 'Unreliable Entity List' regime, under which foreign entities or individuals that boycott or cut off supplies to Chinese companies for non-commercial purposes, causing serious damages to Chinese companies, would be listed as 'Unreliable Entities'.

Lawyers at international law firm Baker McKenzie noted in a briefing on the development that two senior MOFCOM officials had recently commented: '[T]he government would consider the totality of the circumstances in black-listing a foreign business, including (i) the specific "discriminatory measures" taken by the foreign business against Chinese companies, such as boycotting or cutting off supplies to Chinese companies, (ii) whether these measures are taken for non-commercial purposes and against the market rules and contractual obligations, (iii) the material damage caused to the Chinese companies and the related industries, and (iv) the potential threat to China's national security.'

The lawyers also noted that while the Unreliable Entity List regime seems to only target foreign legal entities and individuals, '[O]ne cannot exclude the possibility of enforcement actions taken against the

continues

China subsidiaries of the listed foreign corporations for similar reasons.’

But, they added: ‘China is still in the process of formulating its first Export Control Law. Strictly speaking, it thus far does not have an “entity list” regime similar to that under the U.S. export control law, which may restrict exports of Chinese origin products or technologies to specified foreign entities. While the Export Control Law is generally expected to be enacted by the end of this year or early next year, it is unclear whether the

Unreliable Entity List regime is intended to impose the same restriction that was originally expected to be included in the new Export Control Law.’

Eyes on the prize

China trade law expert, FTI Consulting’s Johnny Xie told *WorldECR* that the US restriction on Huawei ‘is viewed by China as an embodiment of its overall efforts in restricting China’s rising as a nation,’ and that any retaliatory moves by China should, accordingly, be viewed as being ‘strategic’, and on behalf of

the entire nation, not just ‘an individual company’.

He said that, based on current economic performance and forecasts, ‘China believes time is on her side. Therefore, the longer the tensions persist [the greater will be] China’s ultimate win, and China currently would try her best to avoid any irrational or too violent retaliation against the US.’

He said that a ‘tit-for-tat’ principle will be used by China to defend interests in key areas – hence, the proposed Unreliable Entity List, which he contrasted with the EU blocking statute.

‘[The blocking statute] forbids EU persons from complying with US sanctions. The Unreliable Entity List targets foreign persons directly, and its impact is more keenly perceived.’

Xie suggested that other, asymmetric retaliations are available to China: ‘Beijing could waive income taxes for ICT companies like ZTE and Huawei, intensify ICT R&D and indigenous innovation through fiscal investment and policy incentives, and give the green light to the massive commercial application of 5G in China’s sizeable domestic market.’

Japan threatens export ban on South Korea

The Japanese government is considering imposing export controls on some goods bound for South Korea ‘in an apparent effort to raise pressure on Seoul to help resolve a bilateral dispute over compensation for wartime labour.’ So reports Japan’s Kyodo news agency, which describes the plan as a response ‘to what Tokyo views as Seoul’s failure to address the months-long dispute properly and prevent it

from hurting mutual trust between the two neighbours.’ It has been reported that among those items being considered for control are ‘electronic parts and related materials that can be diverted to military use’.

Last year, South Korean courts ordered a number of Japanese companies to compensate individuals and their families forced into slave labour between 1910 and 1945. Japan says the issue has already been fully

settled under an agreement made in 1965. Attempts to resolve the dispute have reached an impasse.

The Japanese government has already announced that, effective 4 July, Japanese exporters must file applications for the export of fluorinated polyimide, hydrogen fluoride and resistors, which Kyodo describes as essential for the manufacture of semiconductors and displays for ‘smart phones and TVs’.

In addition, it is reported, Japan’s Ministry of Economy, Trade and Industry is ‘seeking to remove South Korea from its “white list” of countries that are considered as posing no security risk and can receive preferential treatment in export procedures.’

South Korea trade minister Sung Yun-mo said that the government intends to file a complaint with the World Trade Organisation if Japan imposes the ban.

US sanctions Ayatollah Khamenei, ‘closing door to diplomatic solution’

President Trump has issued an executive order which empowers him to impose sanctions on a new slew of Iranian targets – including its Supreme Leader, the Ayatollah Khamenei, and its Foreign Minister, US-educated Javad Zarif. Iran has responded that, in so doing, the United States has closed the door to a diplomatic solution to the tensions between the two countries.

The executive order is taken ‘in light of the actions of the Government of Iran and Iranian-backed proxies, particularly those taken to destabilize the Middle East, promote international terrorism, and advance Iran’s ballistic missile program, and Iran’s irresponsible and provocative actions in and over international waters, including the targeting of United States

military assets and civilian vessels.’

It came shortly after Iranian forces shot down a US surveillance drone which, the US claims, was in international airspace at the time it was struck – a claim denied by Iran and Russia, both of which state it was in Iranian airspace. Prior to the drone attack, a number of oil tankers travelling through the Strait of Hormuz were attacked in operations which the US and other governments have attributed to Iranian forces.

The Office of Foreign Assets Control (‘OFAC’) has updated its Specially Designated Nationals And Blocked Persons (‘SDN’) List to include Ali Hosseini Khamenei (without according him his official title of Supreme Leader of Iran). Others designated include eight senior

commanders of the Islamic Revolutionary Guards Corp.

Treasury Secretary Steven Mnuchin said: ‘The President’s order will deny Iran’s leadership access to financial resources and authorises the targeting of persons appointed to certain official or other positions by the Supreme Leader or the Supreme Leader’s Office. Moreover, any foreign financial institution that knowingly facilitates a significant financial transaction for entities designated under this Executive Order could be cut off from the US financial system.’

President Trump tweeted: ‘Any attack by Iran on anything American will be met with great and overwhelming force. In some areas, overwhelming will mean obliteration.’

Join us in
LONDON

THE **WORLDECR** EXPORT CONTROLS AND SANCTIONS FORUM **2019**

Focused on **EXPORT CONTROLS, SANCTIONS** and **NATIONAL SECURITY**



Aline Doussain, Hogan Lovells, and Keith O'Leary, Hitachi Vantara: Above and beyond the call of duty? How much compliance is enough compliance?



Jane Shvets and Konstantin Bureiko, Debevoise: Russia and the EU and US sanctions regimes, discrepancies, and how to manage them for compliance



Rosa Rosanelli, BEC: Interpreting the EU Guidelines for ICPs



Marian Niestedt and Gerd Schwendinger, GvW: The EU and the German blocking statutes and their impact on compliance



Amie Ahanchian and Steve Brotherton, KPMG: Auditing the trade function: Developing a robust export control audit programme can be a gamechanger ...



Tina Carlile, BP: Owning the risk and staying resilient – Key to contemporary compliance is the application of resilience tactics...



Barbara Linney, Baker Hostetler: National security laws and due diligence: CFIUS, FDI Regulation, and the impact on corporate activity



Matt Bell, FTI Consulting: Best practice in winding down a business operating in a jurisdiction hit by sanctions



Genevra Forwood and Sara Nordin, White & Case: How sanctions can impact on arbitration clauses



Satish Kini, Jane Shvets and Konstantin Bureiko, Debevoise: OFAC sanctions and the application of extra-territorial jurisdiction through the prism of recent enforcement cases



Timothy O'Toole, Miller & Chevalier: Going deep: a masterclass on investigations best practice



Warren Bayliss, Rolls Royce: The defence supply chain: risks, challenges and opportunities



Lourdes Catrain, Hogan Lovells: Europe – tightening the reins on foreign investment?



Branislav Aleksic, Fraunhofer: R&D, compliance and beyond: the Fraunhofer experience



Keith O'Leary, Hitachi Vantara: Building a compliance strategy for intangible technology transfers

WorldECR subscribers receive a 15% discount

Earlybird fees currently available

official sponsors

Debevoise & Plimpton

Hogan Lovells

BakerHostetler

GvW Graf von Westphalen

Miller & Chevalier

KPMG

FTI CONSULTING

WHITE & CASE

3-4 OCTOBER 2019, 8 FENCHURCH PLACE, LONDON EC3

DOWNLOAD THE BROCHURE AT [HTTPS://WWW.WORLDECR.COM/CONFERENCE-2019/](https://www.worldecr.com/conference-2019/)

UK seeks stay on Saudi arms block

The UK government has requested that the courts set aside a judgment of the UK Court of Appeal that would put military exports to Saudi Arabia on hold. The judgment coincided with the US Senate's vote to block a \$110bn arms deal signed between President Trump and the Kingdom of Saudi Arabia.

The judgment, which the UK government seeks to stay, constitutes a judicial review of a 2017 victory for the government in the High Court, and concerns 'the lawfulness of the grant by the UK Government of export licences for the sale or transfer of arms or military equipment to the Kingdom of Saudi Arabia, for possible use in the conflict in Yemen.'

The Court of Appeal said it had concluded 'that the process of decision-making by the government was wrong in law in one significant respect:

'Part of the legal test under the Export Control Act 2002, the Export Control Order 2008 and the Common Position adopted by the Member States of the European Union in December 2008, is in what is known as "Criterion 2". This means the exporting state must consider "the recipient country's attitudes" towards the principles of "international humanitarian rights instruments" and international human rights law. Criterion 2 stipulates that Member States: "shall ... deny an export licence if there is a clear risk that the ... equipment might be used in the commission of serious violations of international humanitarian law".'

The court said that the error of law it identified 'concerns one part of the process followed by government in considering



No new Saudi arms export licences while ECJU reconsiders 'the decisions we made about those licences'.

that "clear risk ... of serious violations".

'The government made no concluded assessments of whether the Saudi-led coalition had committed violations of international humanitarian law in the past, during the Yemen conflict, and made no attempt to do so.'

In notes on the case, Brick Court Chambers (to which belongs Martin Chamberlain QC, lead counsel for CAAT, the Campaign Against the Arms Trade which brought the action against the government), said, 'The Court of Appeal... unanimously allowed CAAT's first and central ground of appeal. It held that the question whether there was an historic pattern of breaches of IHL [international humanitarian law] was one which had to be faced. Even if it could not be answered

with confidence in respect of every incident of concern, it was clear that it could properly be answered in respect of many such incidents including most if not all of those that had featured prominently in argument. Such an assessment had at least to be attempted,' adding that without assessments of past violations of international humanitarian law, 'it was impossible to know how much weight to give to high level assurances by the Saudi authorities, which had been relied upon by the Secretary of State in reaching his decision that the "clear risk" test was not met.'

On 20 June (following the Court of Appeal judgment), International Trade Secretary Dr Liam Fox told the House of Commons that in assessing arms export licence applications under the relevant criteria, 'We

have used six strands of information and analysis to inform decisions: analysis of all allegations of breaches of international humanitarian law that are known to us; an understanding of Saudi military procedures; continuing engagement with the Saudis at the highest level; post-incident dialogue, including dialogue with respect to investigations; Saudi public commitments to IHL; and regular IHL assessments based on developments in the conflict in Yemen.

'Each of these strands takes into account a wide range of sources and analysis, including those of a sensitive nature to which other parties, such as non-governmental organisations and the United Nations, do not have access. Taken together, these strands of analysis and information, which are reviewed regularly by the FCO [Foreign & Commonwealth Office] in comprehensive reports to the Foreign Secretary and which engage continuously with the record of the Saudis in relation to IHL, form the basis of the Foreign Secretary's advice to the Secretary of State making licensing decisions.'

Licence to drill down into the detail

The ruling has caused some confusion among exporters as to whether they can or can't continue to export under existing licences. UK military export control expert, Martin Drew told *WorldECR*, 'As I understand it, the Court of Appeal order directs the government to introduce a new process in deciding UK export licences in future, which must include considerations of international humanitarian law. No new export licences

UK 'an outlier'

In May, prior to the judgment, *WorldECR* met with Dr Anna Stavrianakis, senior lecturer in International Relations at the University of Sussex and closely involved with CAAT's suit against the government, who observed that 'Across the board of continental Europe you see moves to restrict arms exports to Saudi Arabia. There are cynical and less cynical interpretations of those commitments, but the commitments, and the restrictions are there. We see the UK and France, in that sense, being outliers within Europe. [Faced with the choice of] siding with the rest of continental Europe or the US [they are choosing the latter.]'

can be granted for the Kingdom of Saudi Arabia ('KSA') and its partners until this new process is in place. And all extant export licences must be reviewed because they were made under a "legally flawed" process.'

The 'crux', he suggested, was that, 'The court does not direct that all current SIELs [standard individual export licences] must be cancelled, or indeed that the decision to issue them was wrong, but that [the UK government] must go away and review them. There appears no timescale set to do this and hence any party that currently has a UK export licence in place can lawfully export those goods pending any future Department of International Trade decision.'

'When the Department of International Trade creates this new process and then reviews these extant licences, the decision of course could go either way. But until that time, exporting with said licences appears lawful under the Export

Control Order 2008.'

This, he said, 'also applies to those currently registered to use OGELs [open general export licences] in that they may continue to use them to export to KSA et al, until they change.'

The ECJU line

Meanwhile, the Export Control Joint Unit ('ECJU') of the UK Department of Trade has announced that it will not be granting new licences for export to 'Saudi Arabia and its coalition partners (UAE, Kuwait, Bahrain and Egypt) which might be used in the conflict in Yemen' – pending its consideration of the implications of the judgment. The ECJU says that exporters 'may continue to export under extant licences [but the ECJU] is... required by the Court to reconsider the decisions we made about those licences.'

In addition, it has stopped new registrations for six open general export licences ('OGELs'):

- PCBs and components for

Links and notes

See the judgment at:

<https://www.judiciary.uk/wp-content/uploads/2019/06/CAAT-v-Secretary-of-State-and-Others-Open-12-June-2019.pdf>

Liam Fox's full statement at:

<https://hansard.parliament.uk/commons/2019-06-20/debates/D9BD8C37-E5A0-4A7E-9959-AC40A0DEE622/ExportLicencesHighCourtJudgment>

The US Senate resolutions on the Saudi arms sale at:

https://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=116&session=1&vote=00179

- military goods
- Export after repair/replacement under warranty (military goods)
- Exports for transfers in support of UK government defence contracts
- Software and source code for military goods
- Technology for military goods
- Military goods: collaborative Project Typhoon

It said: 'Exporters who have already registered for these OGELs may continue to use them to export to Saudi Arabia and its coalition partners, subject to the terms and conditions of the licences. Arrangements will be put in place for future registrations for other destinations permitted by

these OGELs.'

Senate says 'No'

On 20 June, the US Senate passed a series of resolutions which, unless vetoed by the US president, would prohibit the issuance of licences for the export of a slew of military goods to Saudi Arabia, the United Arab Emirates and France, Australia and the United Kingdom related to an arms deal signed with Saudi with a value of \$110bn. The deal had been pushed through by President Trump, who used an emergency provision under the Arms Export Control Act without a congressional review period. The US administration said that a 'heightened threat from Iran' justifies the sales.

Canada imposes sanctions on Nicaragua

Canada's Department of Foreign Affairs has announced that it, 'in coordination with the United States', is imposing sanctions 'in response to gross and systematic human rights violations that have been committed in Nicaragua.'

The sanctions are imposed against 'key members of the Government of Nicaragua under the Special Economic Measures Act.'

The Canadian government said:

'Since April 2018, the Government of Nicaragua has conducted a systematic campaign of repression and state-sponsored violence against public protests and the activities of opposition groups.'

'The Government of Nicaragua's unacceptable conduct has been well-documented by international human rights organizations, including the United Nations

Office of the High Commissioner for Human Rights (OHCHR), the Inter-American Commission on Human Rights (IACHR), Amnesty International, Human Rights Watch, as well as local human rights organisations.'

'Despite progress on the release of political prisoners, Canada remains concerned

by reports of human rights violations. These include violating the right to life, security, free speech, and free assembly. There have also been well-documented reports of extrajudicial killings, torture, and abuse of protestors. To date, those responsible for human rights violations have not been held accountable.'

https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/nicaragua.aspx?lang=eng

WorldECR welcomes your news and feedback. Email the editor at tom.blass@worlddec.com

THE **WORLDEC** EXPORT CONTROLS AND SANCTIONS FORUM 2019

Join us in **D.C.**

Focused on EXPORT CONTROLS, SANCTIONS and NATIONAL SECURITY



Nathan Eilers, Rockwell Automation, and Bryce Bittner, Textron: Not just saying 'No!' Trade compliance as a business enabler and accelerator



Inna Tsimmerman, Marsh & McLennan, and Brad Brooks-Rubin, the Enough Project: Exploring the sanctions/human rights calculus



Peter Liston, Walmart: Routed export transactions – high risk but manageable



Dr Christopher Ford, US State Department: The Trump Administration's approach to non-proliferation and national security



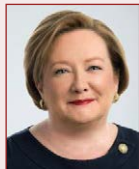
Satish Kini and Carl Micarelli, Debevoise: Understanding OFAC through the prism of its enforcement actions



Amie Ahanchian and Steve Brotherton, KPMG: Auditing the trade function: Developing a robust export control audit programme can be a gamechanger ...



Cyndee Todgham Cherniak, LexSage: Understanding Canadian export controls and how they do and don't differ from those of the US



Barbara Linney, Baker Hostetler: National security laws and due diligence: CFIUS, FDI Regulation, and the impact on corporate activity



Matt Bell, FTI Consulting: Case-study: The life, death and export controls of a crypto-processor – or how to manage export controls across a global supply chain



Marian Niestedt and Dr. Gerd Schwendinger, GvW: The EU and the German blocking statutes and their impact on compliance



Rachel Weise and Tom Gray, Pacific Northwest National Laboratory: Essential links – proliferation finance and export controls



Timothy O'Toole, Miller & Chevalier: Going deep: a masterclass on investigations best practice



Kala Anandarajah, Rajah & Tann, Singapore: The convergence of sanctions, export controls and trade agreements – A multi-jurisdictional case study



Nathan Eilers, Rockwell Automation: A real-time response to sanctions – how his company responded to the escalation of measures against Venezuela



Satish Kini and Carl Micarelli, Debevoise: Exploring the difference between the debt restrictions in the Venezuela and Russia sanctions regimes



Ajay Kuntamakalla, Hogan Lovells, and Bryce Bittner, Textron: Controlling emerging technologies – how will BIS balance innovation and security concerns?

WorldECR subscribers receive a 15% discount
 •
Earlybird fees currently available

official sponsors

Debevoise & Plimpton

Hogan Lovells

BakerHostetler

GvW Graf von Westphalen

Miller & Chevalier

KPMG

FTI CONSULTING

15-16 OCTOBER 2019, HOGAN LOVELLS, 555 13TH ST NW, WASHINGTON, DC

DOWNLOAD THE BROCHURE AT [HTTPS://WWW.WORLDEC.R.COM/CONFERENCE-2019/](https://www.worldecr.com/conference-2019/)

Tank Talk

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

Efforts to prevent proliferation finance ‘in their infancy’

While the US government and Congress have long prioritised reducing the risk of weapons of mass destruction (‘WMD’) proliferation, ‘whether from state actors such as North Korea and Iran, or from non-state actors, particularly criminals and transnational terrorist networks,’ there remains a significant blind spot, argue Elizabeth Rosenberg, Neil Bhatiya, Claire Groden and Ashley Feng in a paper for the Center for New American Security.

‘The efforts to prevent the financing of WMD proliferation are only in their infancy,’ they write. ‘The legal framework to prevent the financing of proliferation is weak, and implementation across the world is spotty. The United States in particular suffers from easily fixable deficiencies in its approach to this critical national security issue.’

‘North Korea and Iran in particular have operated (and North Korea continues to operate) egregious, publicly documented, sophisticated global networks of trusted financial agents. These networks are quite sophisticated at evading detection and know how to

exploit weak regulations and enforcement in jurisdictions around the world.

‘These states are creative and diligent in developing new ways to continually disguise their activities, pioneering new technology and networks to sustain themselves and grow. The United States has prioritized dealing with North Korea and Iran as high-level security threats, but the proliferation finance aspect of that strategy has been woefully underdeveloped.’

Amongst the authors’ recommendations:

‘Congress should pass legislation requiring the reporting to law enforcement of the ultimate beneficial ownership of corporate entities that are created in the United States. Doing so would provide an invaluable tool for information gathering about illicit financial actors, including proliferation networks.’

And, they argue, ‘The existing Customer Due Diligence Rule is insufficient because it only requires certain financial institutions to collect such information, without a mandate that it be automatically transmitted to government authorities.’

<https://s3.amazonaws.com/files.cnas.org/documents/Key-Issues-for-Congress-Proliferation-Finance-final-1.pdf?mtime=20190530085637>

Chinese institutions and universities on entity list – a trade tactic?

Writing in *World University News*, Yojana Sharma describes increased anxiety amongst educational establishments as more and more institutions are added

to the Department of Commerce Entity List.

‘The move by the Bureau of Industry and Security of the US Department of Commerce to add Chinese

institutions to its ‘Entity List’ is seen as a way for the US to protect the transfer of ‘sensitive’ technologies. For some universities it means extra paperwork, while others could be deterred from collaborating with listed Chinese universities or from university-industry collaborations for fear of inadvertently breaking the rules,’ she writes.

The article cites Alex Joske, a researcher at the Australian Strategic Policy Institute, who predicts that more Chinese universities will be added to the list ‘because there’s much

greater attention on US technological competition with China, and the list is being used more and more as a tool,’ and the Executive Director of the Asian Trade Center, Deborah Elms, who says, ‘There are two ways to read the Entity List. One is that it is an attempt by the United States to crack down on institutions on the list. But the second way to read it is that the expansion of the Entity List – and also the inclusion of Huawei – is a negotiating tactic designed to increase the pressure on China to come to the table on the larger trade issues.’

www.universityworldnews.com/post.php?story=20190625091615818

Meeting the challenge of US secondary sanctions in Europe

Secondary sanctions have become a critical challenge for Europe ‘due to the Trump administration’s maximalist policy on Iran and its aggressive economic statecraft.’ European countries should demonstrate that ‘despite their economic interdependence with the US, they control EU foreign policy.’

Such is the argument advanced by Ellie Geranmayeh and Manuel Lafont Rapnouil in a briefing published by the European Council on Foreign Relations which says that the European Union and its Member States ‘should strengthen their sanctions policy, begin to build up their deterrence and resilience against secondary sanctions, and prepare to adopt asymmetric counter-measures against any country that harms European interests through secondary sanctions.’

Amongst the big-ticket

losses caused to European businesses by secondary sanctions it lists:

- \$1.5bn (Siemens losses under a railway contract with Iran)
- \$2bn (Total’s lost investment in the South Pars gas field)
- \$19bn (Airbus losses under contract with Iran Air)

More consistent and credible enforcement mechanisms in the EU could, they argue, ‘provide EU institutions with a more comprehensive overview of the measures and help them put the union’s combined political and economic weight behind exchanges with the US authorities, thereby lending credibility to the deterrent Europeans should aim to establish.’

An alternative, or complementary approach, could be to ‘create other parallel financial channels with limited exposure to the US’.

https://www.ecfr.eu/publications/summary/meeting_the_challenge_of_secondary_sanctions

GERMANY

New directive for military exports

By Fabian A. Jah, Rechtsanwalt
www.der-rechtsanwalt.eu



On 26 June, the German government released a new directive for exports of military items.

The last directive was established in 2000. Such directives are not legally binding. Yet they are guidelines provided by the German Ministry for Economics, which has responsibility for approving exports of military items. (It is worth noting that in Germany, the export of military items is regarded as a privilege, not a right – in contrast to the export of dual-use items which is a right if legal provisions are met, albeit that the government is legally entitled to stop exports of dual-use goods.)

This new directive is more restrictive than its predecessor: The issue of the export of military exports is a very delicate one, given Germany’s history, and it has become more sensitive in the wake of the Khashoggi case, since which the government has stopped the issuance of export licences for military goods to Saudi Arabia. (German industry was already reluctant to use the licences already issued, given the political circumstances.)

So, the German policy toward armament exports is quite ambivalent. Parties from the ‘Left’ are longstanding critics of all exports of military items and proclaim their intention to stop exports of military items. Parties on the

‘Right’ (which no party claims to be – another reflection of history) tend to echo industry’s arguments about the value of defence exports, i.e., as regarding the preservation of jobs, developing technical know-how, industrial competition with other economies, meeting the demands of and obligations toward NATO allies, etc. And, due to Germany’s relatively decreased military spending after the end of the Cold War, there is an argument that without exports, military manufacturing will not be sustainable.

Germany’s policy has been criticised, even by EU partners and NATO allies.

The French government regards Germany’s policy as an obstacle for joint projects on the development of military equipment (e.g., as part of PESCO projects to strengthen cooperation and the integration and harmonisation of EU Member States’ military equipment).

The German military industry trade association (‘BDSV’) has criticised the new directive – especially as regards its prohibition of exports of small weapons to non-EU/non-NATO (with exceptions for Switzerland, Japan, Australia, New Zealand) countries.

Indeed, many in both politics and industry had concerns that the

previous directive had hindered PESCO projects.¹ The new directive does refer to PESCO, but takes a different line, expressly stating that the German government should counter exports of PESCO partners that are not aligned with German export standards.

On the other hand, the directive speaks of:

- A (yet-to-be-established) *de minimis* regulation for supplies of compounds to EU and NATO countries;
- Intensification of so-called ‘post-shipment’ checks;
- Better supervision of re-exports;
- Strengthening of human rights as a criterion for approving exports;
- Greater controls on technologies that could be used to build up production capacities abroad (due to the German government’s wavering policies on arms exports, some companies have taken to establishing factories abroad).

Links and notes

The guidelines are at:
<https://www.bmwi.de/Redaktion/DE/Dossier/ruetzungsexportkontrolle.html>

¹ [https://eeas.europa.eu/headquarters/headquarters-homepage_en/34226/Permanent%20Structured%20Cooperation%20\(PESCO\)%20-%20Factsheet](https://eeas.europa.eu/headquarters/headquarters-homepage_en/34226/Permanent%20Structured%20Cooperation%20(PESCO)%20-%20Factsheet)



THE WORLDECR SEARCHABLE ARCHIVE

The WorldECR Archive at www.worlddecr.com includes all past journal and website news PLUS every article that has ever appeared in WorldECR.

If you would like to find out more about Archive Access, contact Mark Cusick, WorldECR’s publisher at mark.cusick@worlddecr.com

BRAZIL

Brazil enacts regulations on enforcement of international sanctions

By Vera Kana, TozziniFreire Advogados

tozzinifreire.com.br



A new Decree No. 9,825, dated 5 June 2019, has been published in Brazil's *Official Gazette*, and provides for measures on enforcement of sanctions against persons investigated or accused of terrorism, its financing or related acts.

The Decree includes sanctions imposed by resolutions of the UN Security Council as well as by other countries, or even as imposed by Brazilian authorities.

Sanctions may be applied against individuals, companies or any other entities, and may include:

- Import or export restrictions;

- Blocking of assets – that is, prohibitions to transfer, convert, dispose or make assets available, directly or indirectly; and
- Restrictions on entering or leaving Brazil.

The Decree highlights the central role of the Department of Asset Recovery and International Legal Cooperation of the Ministry of Justice and Public Security, in coordination with other regulatory and oversight agencies, for adopting the necessary measures to comply with sanctions. The Department will also publish lists of natural persons, legal entities and

entities subject to sanctions, reinforcing the necessity to review applicable Brazilian and international regulations and sanctions on a case-by-case basis on imports and exports operations.

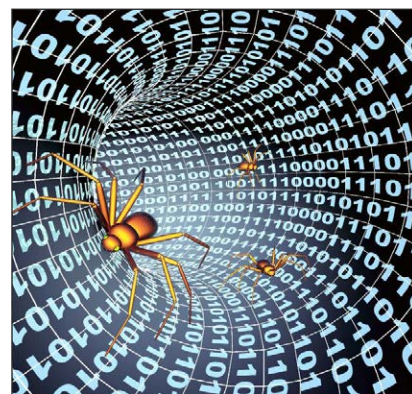
This new Decree can be seen as part of a movement to expand and consolidate the application of sanctions in Brazil, including economic sanctions, which demonstrates the importance of implementing solid trade compliance controls, considering the potential for damages (including, and especially, reputational) for persons and companies sanctioned in case of non-compliance with measures imposed by other countries and Brazil.

EU

EU introduces a sanctions regime targeting cyber-attack

By Nadya Nychay, Nicoleta Tuominen and Laurens Engelen, Dentons

www.dentons.com



Following years of legislative debate, on 17 May 2019 the European Union adopted a legal framework setting out

sanctions targeting persons and entities responsible for significant cyber-attacks aiming to undermine the integrity, security and economic competitiveness of the EU. The framework and the new sanctions regime are set out in Council Decision 2019/797 ('the Decision') and Council Regulation (EU) 2019/796 ('the Regulation').¹

Support for the new regime has been declared by a number of third countries, i.e., Turkey, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Norway, Moldova and

Georgia, which joined the EU High Representative's declaration of 12 April 2019 on respect for a rules-based order in cyberspace. It now remains to be seen how many of these countries will follow through and use the momentum to enact their own legislation targeting cyber-attacks.

How does the sanctions regime define a cyber-attack?

The Decision and Regulation define a cyber-attack as any action involving access to information systems, information systems interference, data interference or data interception that

Links and notes

¹ Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129, 17.05.2019, p. 13) and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129, 17.05.2019, p. 1).

² Critical infrastructure is that which is essential for the maintenance of vital functions of society, or the health, safety, security and economic or social well-being of people.

is not authorised by the owner or holder of the relevant rights of the system or the data, or which is illegal under the laws of the relevant Member State. To fall under the scope of the relevant legislative framework, a cyber-attack must (1) be an external threat to the interests of the EU or its Member States, and (2) have a potentially significant effect.

When are the EU’s or its Member States’ interests affected by an external threat?

The legal framework against cyber-attacks identifies three sets of external threats that could trigger an EU response; i.e., a threat to EU interests, a threat to Member State interests, and a threat to certain third states or international organisations.

Pursuant to the EU sanctions framework, the EU’s interests are threatened if a cyber-attack is carried out against its institutions, bodies, offices and agencies, international delegations, security and defence operations and missions as well as special representatives.

Member State interests are

threatened when cyber-attacks are committed against critical infrastructure,² services that are necessary for maintaining essential social and/or economic activities,³ critical state functions,⁴ storage or processing of classified information or government emergency response teams. Furthermore, cyber-attacks against third states or international organisations can also be caught under the scope of the measures to the extent that is necessary to achieve the EU’s common foreign and security policy objectives.

To qualify as an external threat, the cyber-attack must either originate or be carried out from outside the EU, or by using non-Union infrastructure, or be carried out by persons or entities established or operating outside the EU, or carried out with the support or under the control of anyone outside the EU.

When does a cyber-attack have a potential significant effect?

As noted, the EU seeks to target cyber-attacks that have a potentially significant effect. The specific factors

determining whether a cyber-attack has a potentially significant effect are:

- Scope, scale, impact or severity of the disruption caused, including to economic and social activities, essential services, critical state functions, public order or public safety;
- Number of natural or legal persons, entities or bodies affected;
- Number of Member States concerned;
- Amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
- Economic benefit gained by the perpetrator, for himself or for others;
- Amount or nature of data stolen or the scale of data breaches;
- Nature of commercially sensitive data accessed.

What sanctions can be imposed under the new anti-cyber-attacks measures?

The Decision and the Regulation allow the imposition of a travel ban and an

Embargos and Sanctions
 „Leading foreign trade law practice in Germany“
 (JUVE Handbook 2015/2016)

Graf von Westphalen
 Attorneys-at-law and Tax Advisors

Berlin Düsseldorf Frankfurt Hamburg Munich
 Brussels Istanbul Shanghai

Contact:
 Dr Lothar Harings, l.harings@gvw.com
 Marian Niestedt, M.E.S., m.niestedt@gvw.com gvw.com

GW Graf von Westphalen

asset-freeze against persons deemed responsible for cyber-attacks, and enables a ban on funds or economic resources to be imposed on those persons. It should be noted that these measures may not only be imposed against those deemed directly responsible for an actual or attempted cyber-attack. Persons and entities

having provided support or participated in the planning of the cyber-attack, as well as persons and entities associated with those responsible, can also be targeted.

The relevant list of targeted persons and entities is annexed to the Regulation and the Decision. At the moment, the list is still empty. The

Council of the EU is authorised to list and delist persons and entities by acting in unanimity upon a proposal by a Member State or the EU High Representative for Foreign Affairs and Security Policy. As with all other EU restrictive measures, the anti-cyber-attacks sanctions will also be enforced by the Member States.

HONG KONG

Implementation of United Nations Security Council sanctions

By Alan H. Linning, Susanne J. Harris and Zoe A. Keane, Mayer Brown

www.mayerbrown.com



On 23 January, The Hong Kong government, via Acting Secretary for Commerce and Economic Development Dr Bernard Chan and in response to a query from a lawmaker (the Hon. Kenneth Leung), published a press release in which it revealed the number of sanctions investigations and related enforcement actions undertaken by the Hong Kong government relating to potential breaches of United Nations Security Council (‘UNSC’) sanctions over the past five years, as well as detailing staffing levels dedicated to such investigations. The publication confirmed that the governmental departments enforcing the United Nations Sanctions Ordinance (Cap 537) (the ‘Ordinance’), comprise

- i) the Hong Kong Police Force (‘HKPF’) and
- ii) the Customs and Excise Department (‘C&ED’).

It states the workload of 69 staff in HKPF and 47 staff in C&ED includes enforcement review and action arising out of the Ordinance. A more detailed breakdown of manpower for each duty concerned was not available, however.

It also confirmed that investigations by HKPF had increased, from three in 2014 to 201 in 2018, and that those by the C&ED had increased from 10 to 99 during the same period. Whilst there has been a clear rise in the number of sanctions investigations, there has been no explanation for the cause of the uptick. The press release also confirmed that there have been no prosecution cases brought under the Ordinance to date.

Notwithstanding the lack of prosecutions, it said, ‘Hong Kong has a robust system to implement sanctions imposed by the UNSC,’ and that the agencies’ investigation efforts act as a deterrent to potential violators. In that regard, the press release notes that a number of Hong Kong-registered companies have been struck off and certain vessels denied entry into Hong Kong waters, and that these actions are deterrents to those considering using Hong Kong as a base from which to violate UNSC sanctions.

It said that the agencies actively investigate all suspected violations of

UNSC sanctions ‘without fear or favour’ and would prosecute where sufficient evidence was available.

The press release emphasised the Hong Kong government’s commitment to upholding UN sanctions, adding that whilst countries are able to impose unilateral sanctions, the Hong Kong government ‘does not have the responsibility nor the authority to enforce these unilateral sanctions or investigate related cases.’¹

These comments are particularly pertinent in light of the arrest of Huawei’s Chief Financial Officer Sabrina Meng Wanzhou at the request of US authorities on allegations of the company’s dealings with UNSC-sanctioned Iran through a Hong Kong shell company.

Hong Kong’s Deputy Secretary of Commerce and Economic Development Bureau Vivian Sum Fong-Kwang recently told legislators that ‘Hong Kong is not obliged to enforce sanctions imposed by the United States,’ and ‘the city government would only act on sanctions ordered by the UN Security Council, and would not enforce unilateral sanctions by individual jurisdictions, including the US or the European Union.’² It is not yet clear whether the allegations against Meng Wanzhou and Huawei could fall under the UNSC restrictions.

Additional sanctions-related media coverage for the Hong Kong government came in the form of a

Links and notes

- ¹ <https://www.info.gov.hk/gia/general/201901/23/P2019012300436.htm>
- ² <https://www.scmp.com/print/news/hong-kong/politics/article/2177712/hong-kong-not-obliged-enforce-sanctions-imposed-us-alone>
- ³ <https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2157877/lawsuit-filed-over-failure-hong-kong>

This article was originally published in the Perspectives & Events section of the website of Mayer Brown and is reproduced with permission. All rights reserved to Mayer Brown. The contents of this article are intended to provide a general guide to the subject matter and should not be treated as a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein. For further information please contact the authors or Mayer Brown partner Tamer Soliman at tsoliman@mayerbrown.com

Hong Kong-registered vessel having been detained by South Korean authorities in November 2017 for alleged transfer of oil to the Democratic People's Republic of Korea, also subject to the UNSC sanctions regime. The case is now the subject of judicial review proceedings, due to be heard in early 2019.³

Evidently there has been an

increased effort by the Hong Kong government to tackle potential breaches of UNSC sanctions over the past five years. Given the increased focus on sanctions enforcement, both at home and internationally, and particularly in light of the ongoing case involving Huawei, there will no doubt continue to be increased scrutiny on the Hong Kong government's actions in

the sanctions space. It is likely the government will continue to increase its efforts in deploying deterrent tactics and strengthening its enforcement capabilities and, given the number of UNSC sanctions investigations has been significantly trending upwards, Hong Kong could at some point also see the first prosecution brought under the Ordinance.

USA

Russia facing more sanctions

By John E. Smith, Morrison & Foerster

www.mofo.com



February this year saw the introduction of the Defending American Security from Kremlin Aggression Act, or 'DASKA',¹ a bipartisan effort to impose new sanctions on Russia. Interest in action against the Kremlin has only increased following the Mueller Report's release, with Congress now considering no fewer than five Russia-focused sanctions bills. The latest of the bunch explicitly threatens the Nord Stream 2 gas pipeline project, sanctions against which US Energy Secretary Rick Perry says are inevitable:

'The opposition to Nord Stream 2 is still very much alive and well in the United States,' Perry said during a visit to Kiev on 21 May 2019, according to media reports. 'The United States Senate is going to pass a bill, the House is going to approve it, and it's going to go to the President, and he's going to sign it, that is going to put sanctions on Nord Stream 2.'

That threat in particular is sending shockwaves across Europe, as German Chancellor Angela Merkel has publicly supported Nord Stream 2 as vital to Germany's energy security. This is not the first time Nord Stream 2 has been in congressional crosshairs; in 2017, Congress passed the Countering America's Adversaries Through Sanctions Act (CAATSA),² which included a provision that allows the administration to target certain high-value investments or sales for the

construction of Russian energy export pipelines. That authority, however, is discretionary, and its implementing agency, the US State Department, subsequently issued guidance³ indicating that only projects initiated

Interest in action against the Kremlin has only increased following the Mueller Report's release, with Congress now considering no fewer than five Russia-focused sanctions bills.

after CAATSA's enactment would be subject to sanctions, thereby effectively excluding Nord Stream 2 and easing tensions with Germany and others. The latest bill, which calls for mandatory sanctions, leaves no room for similar diplomatic manoeuvring.

With so many bills circulating and so much at stake for business interests around the world, we have prepared a brief primer on each bill, with the caveats that additional bills and amendments are likely forthcoming and the legislative timeline remains unclear. Note that many of the bills contain overlapping features that would require sanctions against Russian energy projects, oligarchs, and newly issued sovereign debt – an

indication that measures related to these sanctions targets will likely make it into whatever ultimately becomes law.

The Protecting Europe's Energy Security Act of 2019 ('PEESA')⁴ – filed on 14 May 2019 by senators Cruz, Shaheen, Barrasso, and Cotton – would require the Secretary of State to issue a report within 60 days, and every 90 days thereafter, on (1) vessels that engaged in pipe-laying at depths of 100 feet or more below sea level for the construction of Russian energy export pipelines; and (2) foreign persons that have sold, leased, provided, or facilitated the provision of those vessels for the construction of such pipelines. As a result of being identified in any of the reports, the following sanctions would result in:

- The assets subject to US jurisdiction of any foreign persons (individuals or entities) identified in (2) above would be required to be blocked (or frozen);
- The corporate officers and principal shareholders of any company owning a vessel identified in (1) above, as well as any foreign persons identified in (2) above, would be denied visas and prohibited from entering the United States; and
- A menu of possible sanctions, including asset-freezes, could be imposed on any foreign persons that

provided underwriting services or insurance or reinsurance for a vessel identified in (1) above, as well as on the corporate officers of any such companies.

The bill would provide the administration with authority to waive the application of sanctions based on national security considerations, but in the current political climate, such a waiver would be extremely difficult for the administration to issue. The bill also calls for a report within six months and annually thereafter (1) listing all entities, including financial institutions, that directly or indirectly provided goods, services, or technology for the construction or repair of the Nord Stream 2 pipeline and (2) assessing whether such entities had knowingly engaged in a ‘significant transaction’ with a sanctioned Russian party. Any positive assessment presumably would force the administration into imposing sanctions against any such entity, given that CAATSA requires that such significant transactions result in mandatory secondary sanctions.

As with CAATSA, much of the bill is phrased neutrally in terms of ‘Russian energy export pipelines’, but the sponsors are clearly focused on Nord Stream 2. ‘Nord Stream 2 threatens Europe’s energy security,’ senator Cruz noted⁵ upon the bill’s filing. ‘The United States simply cannot allow Russia to dominate Europe’s energy future.’

The Defending Elections from Threats by Establishing Redlines Act of 2019 (‘DETER’)⁶ – introduced 8 April 2019 by senators Van Hollen and Rubio – would require (1) determinations and reports to Congress by the Director of National Intelligence (‘DNI’) within 60 days of a US election on whether, with a high level of confidence, a foreign government or agent of a foreign government knowingly interfered in the election; (2) annual reports to Congress providing information on Russian oligarchs, senior political figures, and parastatal entities; and (3) biannual reports to Congress on the wealth, sources of wealth, and use of wealth of such persons, including Russian President Putin. As sanctions

watchers recall, it was a similar provision of CAATSA that resulted in the extraordinary sanctions against Russian oligarchs in April 2018 whose effects were (and continue to be) felt around the world.

If the DNI determines under (1), above, that Russia or a Russian agent interfered in an election, the United States must, within 30 days of that determination, impose the following sanctions:

- Blocking and/or correspondent account sanctions on at least two of the following major Russian banks: (1) Sberbank; (2) VTB Bank; (3) Gazprombank; (4) Vnesheconombank (VEB); and (5) Rosselkhozbank;
- Prohibitions on new investments in the Russian energy sector, including blocking sanctions on any foreign person (individual or entity) that makes a new investment in the Russian energy sector or a Russian energy company;
- Blocking and visa sanctions on Russian senior political figures and oligarchs determined by the DNI to





EXPORT COMPLIANCE
TRAINING INSTITUTE

www.LearnExportCompliance.com



“US Export Controls on Non-US Transactions”

NEW EAR & ITAR Definitions and all Reform Changes

EAR / ITAR & OFAC COMPLIANCE FOR NON-US COMPANIES

COMING TO:

AMSTERDAM

SEPT/OCT 2019

●

SINGAPORE

APRIL 2020

●

LONDON

MAY 2020

- Persons and Items Subject to US Jurisdiction (ITAR, OFAC & EAR)
- Evolving Sanctions
- Trump Administration Regulation and Enforcement Priorities
- Technical Data Considerations
- Enforcement Issues, Practical Advice...and MUCH MORE

Visit www.LearnExportCompliance.com/schedule
or call +1 540 433 3977 (USA) for details or registration

SPEAKER PANEL



Greg Creeser
ITC Strategies



Scott Gearity
BSG Consulting



Marc Binder
ITC Strategies

have directly or indirectly contributed to the election interference;

- Blocking sanctions on entities that are part of, or operate on behalf of, the Russian defence or intelligence sectors; and
- Prohibitions on all transactions in (1) sovereign debt of the Russian government issued after the enactment of DETER and (2) debt of any entity owned or controlled by Russia issued after the enactment.

The bill would provide the President with limited power to waive or suspend sanctions. The President may waive sanctions (except with respect to senior political figures and oligarchs) by certifying that (1) the waiver is in the vital national security interest of the United States; and (2) failing to use the waiver will cause significant adverse harm to the vital national security interests of the United States. The President may suspend sanctions if the DNI certifies that the Russian government has not engaged in interference in US elections for at least one federal election cycle. Should Russia, after any suspension of sanctions, fail to show there is improved government oversight of and prosecutions relating to interference in US elections and credibly demonstrate a significant change in behaviour and credibly commit to not engaging in such interference in the future, the President must reimpose sanctions.

The Defending American Security from Kremlin Aggression Act ('DASKA') – introduced on 13 February 2019 by senators Graham, Menendez, Gardner, Cardin, and Shaheen – would

confront the Kremlin on a range of issues, including Russia's continued interference in democratic processes in the United States and abroad, malign influence in Syria, continued aggression toward Ukraine, and support of criminal organisations and other malicious actors in cyberspace. The bill runs for 119 pages, contains provisions dealing with all sorts of Russian (and non-Russian) policy measures, and would require:

- Sanctions on any person that knowingly makes a new large

DASKA also would require the Secretary of State to determine, within three months, whether Russia is a state sponsor of terrorism.

investment in a liquefied natural gas ('LNG') export facility outside Russia or any energy project outside Russia 'supported by' a Russian parastatal entity or an entity owned or controlled by the Russian government;

- Sanctions against the sale, lease, or provision of high-value goods, services, technology, financing, or other support, including infrastructure repair or modernisation, which significantly contributes to the Russian government's development and production of crude oil resources in Russia (but would not apply to efforts to maintain projects ongoing on the date of DASKA's enactment);
- Sanctions on Russian oligarchs linked to President Putin who facilitate bad acts on his behalf;
- Prohibitions on US persons from dealing in new Russian sovereign debt – including bonds issued by, and foreign exchange swap agreements with, the Russian Central Bank, National Wealth Fund, or Federal Treasury – exceeding 14 days' maturity;
- Sanctions on Russian financial institutions that provide financial or other support for Russian government interference in democratic processes outside Russia; and

- Mandatory quarterly determinations by the Secretary of State on whether the Russian government was interfering with freedom of navigation anywhere in the world, and if so, would require sanctions against all entities operating in the Russian shipbuilding sector.

DASKA also would require the Secretary of State to determine, within three months, whether Russia is a state sponsor of terrorism, which – in the event of an affirmative determination – would result in additional sanctions and export restrictions. It also would incorporate the International Cybercrime Prevention Act ('ICPA')⁷, which has been introduced in Congress in various forms since 2015 and seeks to raise the costs on malicious cyber activity. The bill would create additional authorities to seize botnets and prohibit cyber criminals from selling access to botnets to carry out cyber attacks – seeking to build on the US government's successful disruption of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014, both of which emanated from Russia.

The bill also contains long-discussed beneficial ownership provisions to require domestic title insurance companies to obtain, maintain, and report information on beneficial owners of entities that purchase high-value residential real estate in the United States. This requirement is similar to FinCEN's temporary geographic targeting orders that require companies to collect and report beneficial ownership and other ownership information for all cash transactions exceeding \$300,000 by legal entities for real estate located in specific metropolitan areas in Texas, Florida, New York, California, Hawaii, Nevada, Washington, Massachusetts, and Illinois.

A Bill To Respond to and Deter Russian Attacks on the Integrity of United States Elections⁸ – discussed at a House hearing on 15 May 2019 but not yet introduced – would require:

- Within 90 days of enactment, blocking sanctions against any energy project located outside Russia, where the Russian government or a Russian parastatal invests more than \$5 million after a 90-day period after enactment;
- Within 90 days of enactment, blocking sanctions against any

Links and notes

¹ <https://www.congress.gov/116/bills/s482/BILLS-116s482is.pdf>
² https://www.treasury.gov/resource-center/sanctions/Programs/Documents/hr3364_pl115-44.pdf
³ <https://www.state.gov/caatsa-crisea-section-232-public-guidance/>
⁴ <https://www.congress.gov/116/bills/s1441/BILLS-116s1441is.pdf5>
https://www.cruz.senate.gov/?p=press_release&id=4474
⁶ <https://www.congress.gov/116/bills/s1060/BILLS-116s1060is.pdf>
⁷ <https://www.congress.gov/bill/116th-congress/senate-bill/482/text?q=%7B%5B%22international%22%5D%7D&rs=2#toc-id10F125618FBE42A2826B31DE3B988FE0>
⁸ <https://docs.house.gov/meetings/BA/BA10/20190515/109498/BILLS-116pjh-deterrussia-U1.pdf>

Russian financial institution or Russian person that assisted with election interference by the Russian government in the 2016 or 2018 US elections;

- Within 60 days of enactment, prohibitions on US persons from transacting with, financing, or otherwise dealing in Russian sovereign debt issued at least 90 days after enactment;
- Within 90 days of enactment, requirements on US persons to disclose equity interests in large Russian banks (Vnesheconombank (VEB), Sberbank, VTB Bank,

Gazprombank, Rosselkhozbank, and Promsvyabank).

For future elections, the DNI would be required, within 60 days of a US election, to report to Congress with a high level of confidence whether the Russian government or a Russian agent knowingly interfered in an election. If so, the following sanctions would be required:

- New sanctions on one or more of the six Russian financial institutions listed above or on the Russian Direct Investment Fund;

- Prohibitions on new US investments in the energy sector of Russia or Russian energy companies;
- Sanctions on any foreign person that makes a new investment in Russia's energy sector or energy companies owned by Russia;
- Blocking sanctions on all defence firms owned by Russia, including Rostec.

These bills are the latest word in the ongoing conversation in Congress about how to deal with Russia and an administration oft-criticised for not taking a harder line against the Kremlin.

USA

US imposes sanctions on Iranian government officials, Supreme Leader

By Michael T. Gershberg, Justin A. Schenck and Avani Uppalapati, Fried Frank

www.friedfrank.com



On 24 June 2019, President Trump issued an executive order ('EO') imposing new sanctions on Iranian government officials. The EO prohibits transactions with the Supreme Leader of Iran, Ayatollah Ali Khamenei, his office, any government officials appointed by the Supreme Leader, and any directors or officers of designated entities. The EO also authorises secondary sanctions against foreign financial institutions that conduct significant transactions with the newly blocked persons.

These new sanctions will have

minimal effect on US businesses, which are already broadly prohibited from dealing with Iran. However, they are intended to further pressure Iranian leadership and third countries that deal with Iran. The EO directly designates the Iranian Supreme Leader as a blocked person, and authorises OFAC to designate as blocked persons other Iranian government officials and anyone who provides material support to the Supreme Leader's office.

If any foreign financial institution knowingly conducts or facilitates any significant transaction related to the

designated persons, it may be barred from opening any correspondent or payable-through accounts in the United States. In addition to the financial sanctions, the EO also blocks the entry of designated persons into the United States.

The White House issued a press release stating that these actions were a response to recent Iranian aggression towards the United States, including the downing of a US drone. President Trump stated that the sanctions are also aimed at stemming Iran's sponsorship of terrorism. He said '[T]hese measures represent a strong and proportionate response to Iran's increasingly provocative actions.'

They come only a few weeks after the imposition of additional sectoral sanctions and are the latest in a series of measures to pressure Iran to reduce its nuclear threat. All US companies and any financial institution that conducts business internationally, particularly any companies that do business with Iran, should thoroughly review their business activities and ensure compliance with these new sanctions. Companies should also update their compliance policies and procedures to reflect the latest changes.



Included with this issue of WorldECR

US SANCTIONS AND ENFORCEMENT

A special report

Lacking substance

'There is literally nothing true in this tweet.'

So (tweeted) a highly experienced sanctions analyst and adviser of the US president's claim that

'Iran has long been secretly "enriching," in total violation of the terrible 150 Billion Dollar deal made by John Kerry and the Obama Administration. Remember, that deal was to expire in a short number of years. Sanctions will soon be increased, substantially!'

(The adviser may have made an exception for the last sentence.) But the reality is that the International Atomic Energy Agency has verified Iran's compliance with the terms of the JCPOA from the outset and the US president has not yet divulged the source of his 'secret enrichment' claim; the value of Iranian assets unfrozen by

the JCPOA is estimated at less than one-third of \$150bn, and the deal is subject to oversight by a joint

The International Atomic Energy Agency has verified Iran's compliance with the terms of the JCPOA since implementation day.

commission for 25 years after implementation day.

The current tensions in the Gulf of Hormuz, and Iran's (pointedly not secret) threats to resume enrichment beyond the agreed measures, are regrettable. But they are not surprising to the very many supporters of the nuclear deal, and the painstaking

diplomatic process that lead up to it. Nor, perhaps, are they surprising, or even undesirable, to those who were pleased by the US government's abrupt reversal of its own position. The question is not, Are there agendas at work? But, rather: What and whose are they? It is to be hoped that history doesn't find itself obliged to scrutinise the question too closely, too soon.

All the while, the United Kingdom is looking increasingly orphaned by a combination of its own pursuit of ever-chimeric 'sovereignty', and the unfortunate leak of a diplomatic (?) appraisal of the current administration of its 'closest ally'. Watershed moments? Maybe, but there are more down the road.

The ways forward?

WorldECR has been canvassing the thoughts of its constituents around the world. How are sanctions affecting their businesses? How easy is it to take steps that anticipate change? Is there buy-in for the underlying objectives of sanctions policy? And how well equipped are the regulatory agencies, to manage the workload that they create for themselves?

Here are some thoughts:

- Sanctions and export controls are 'converging' – at least, in the perceptions of those tasked with managing compliance. The addition of Huawei to the entity list (TGL, Trump tweet etc. notwithstanding) was seen as a *de facto* sanction.
- US policy divergence from the UN/EU is now regarded as complete. The direction of travel of one is little indication as to what the other might do. And there is an impression that sanctions are 'being used for purposes for which they were not originally designed' – in other words, redesigned, according to an uncertain blueprint.

Agree or disagree with these characterisations? Please let us know! We welcome all thoughts on the law, politics and practice of every element of trade controls (so long as they have substance.)

Tom Blass, July 2019
TNB@worlddecr.com



EAR/OFAC EXPORT CONTROLS, ITAR DEFENSE TRADE CONTROLS
AND **General Awareness** e-SEMINARS AVAILABLE

Modules for **US** and **Non-US** Companies

Now it is easier than ever to get the best training on complying with EAR, ITAR and OFAC regulations and sanctions without the time and travel cost of being out of the office.

Train on YOUR computer at YOUR convenience!

- * **Video Instruction**
- * **Key Concept Powerpoint Slides**
- * **Comprehensive & Searchable e-Manual**
- * **Optional ECoP® Certification Testing**

www.LearnExportCompliance.com/e-Seminars

New US sanctions aim to cripple Cuba's economy



The recent raft of US sanctions on Cuba are driven by President Trump's desire to keep hold of the conservative Cuban American vote and secure regime change on the island, writes Professor William M. LeoGrande. But, he argues, any change in the White House itself could see that position change over night.

Since winning the White House, President Donald Trump has imposed a series of escalating economic sanctions against Cuba aimed at crippling the economy, fomenting unrest, and ultimately bringing down the government. Relations have gone from bad to worse and there is no reason to expect any improvement so long as Trump remains in the White House.

Trump believes¹ he won Florida in 2016 because of Cuban American votes, and he thinks punishing Cuba can deliver that critical state again in 2020. During the 2016 campaign, he promised to reverse President Barack Obama's opening to Cuba and six months after inauguration, he announced² to a crowd of conservative Cuban Americans in Miami that he was 'cancelling' Obama's policy of engagement. With rhetoric reminiscent of the worst moments of the Cold War, Trump declared a return to the policy of regime change, saying, 'With God's help, a free Cuba is what we will soon achieve.'

However, rhetoric aside, the sanctions announced in June 2017 were relatively mild. Trump ended individual travel to Cuba for educational purposes, but still allowed group educational travel. He banned transactions with certain Cuban firms managed by the armed forces, but otherwise, commercial relations and government to government cooperation continued uninterrupted. Most of the architecture of engagement built by Obama was left intact.

That outcome was a compromise. The White House, strongly influenced³ by Senator Marco Rubio and hardline Miami exiles, favoured radical new sanctions against Cuba from the very beginning. 'Make Rubio happy,' Trump instructed⁴ his staff. But most of the US government bureaucracy concluded that the opening to Cuba improved

cooperation on issues of mutual interest, and they resisted any reversal. They were reinforced by the US business community, which was eager

With rhetoric reminiscent of the worst moments of the Cold War, President Trump declared a return to the policy of regime change.

to take advantage of the Cuban market. For a few months, it looked like relations might stabilise.

In August 2017, however, the revelation of mysterious health problems⁵ suffered by some two dozen US diplomats in Havana gave conservatives an opportunity to re-

open the sanctions debate. Responding to Sen. Rubio's demands, the State Department drastically reduced the staff at the US embassy and forced an equal number of Cuban diplomats out of Washington. Secretary of State Rex Tillerson issued a travel advisory warning US residents not to visit Cuba, and in the first half of 2018, the number of US visitors plummeted⁶ by 23.6%.

The embassy staff reductions were made permanent⁷ in March 2018. Reduced operations severely damaged cultural and educational exchanges, commercial relations, and cooperation on issues of mutual interest. The US embassy stopped processing Cuban visas for travel to the United States and, as a result, Washington failed to meet its commitment under the 1994 migration agreement to provide a minimum of 20,000 immigrant visas to Cubans annually. With skeletal



staffs, the two embassies are barely functioning today.

From Caracas to Havana

As the political crisis in Venezuela has intensified, the Trump administration has blamed Havana for the Venezuelan opposition's failure to oust Nicolas Maduro. The White House has used Cuba's support for Maduro as a rationale for imposing yet another round of sanctions. This new strategy coincided with changes in the White House staff. John Bolton, who targeted Cuba during George W. Bush's administration with unsubstantiated claims⁸ that Havana was developing biological weapons, became Trump's national security advisor in April 2018. In September, Bolton hired Mauricio Claver-Carone, a long-time lobbyist for hardline policies toward Cuba, as senior director for Western Hemisphere Affairs at the National Security Council.

Speaking in Miami on the eve of the 2018 US mid-term elections, Bolton ratcheted up⁹ the rhetoric, calling Cuba, along with Venezuela and Nicaragua, a 'Troika of Tyranny', 'triangle of terror,' and the 'Three Stooges of socialism'. He accused Cuba of 'vicious attacks' on US diplomats in Havana, even though investigators have been unable to determine the cause of their injuries. He promised escalating sanctions to overthrow all three governments. 'The United States now looks forward to watching each corner of the triangle fall,' he declared.

The Venezuelan opposition has promised to cut off the 40,000 barrels of oil¹⁰ Cuba receives daily from Venezuela as payment for medical services, and Washington has already imposed financial sanctions¹¹ against companies transporting Venezuelan oil to Cuba. Depriving Cuba of Venezuelan oil, US officials believe, will cause an economic collapse and popular uprising. The loss of Venezuelan oil would certainly be a blow to the Cuban economy. Economist Pavel Vidal estimates¹² that it would reduce Cuba's gross domestic product by four to eight percentage points, or somewhat more if the cut-off was abrupt. That would be painful, but far short of the 35% decline Cuba survived during the Special Period in the 1990s. Over the past two years, Cuba has managed to absorb a 50% drop¹³ in Venezuelan oil shipments without sinking into recession.

The long Arm of the law: Helms-Burton's extraterritorial sanctions

On 17 April 2019 – the anniversary of the failed Bay of Pigs invasion – Secretary of State Mike Pompeo announced that the Trump administration would allow Title III¹⁴ of the Cuban Liberty and Democratic Solidarity Act (Helms-Burton) to go into effect. Suspended by every other president since the law was passed in

The White House has used Cuba's support for Venezuela's President Nicolas Maduro as a rationale for imposing yet another round of sanctions.

1996, Title III allows US nationals who lost property after the 1959 revolution, including Cuban Americans, to sue Cuban, US, or foreign companies in US federal court for 'trafficking' in their confiscated property – that is, making commercial use of it.

The US Foreign Claims Settlement Commission has certified 5,913 claims¹⁵ of US nationals whose property was seized. These are claims that Cuba recognises and that the United States and Cuba had begun to discuss during the Obama administration. But Title III takes the unusual position of allowing naturalised Cuban Americans who lost property to also file suit against alleged traffickers. According to the Department of State, by including Cuban Americans who were not US citizens when their property was taken, Title III creates the potential for an estimated 75,000-200,000 claims

worth 'tens of billions of dollars'.¹⁶

International law recognises the sovereign right of governments to dispose of the property of their own citizens. For US courts to sit in judgment of another government's actions towards its own citizens in its own territory is a challenge to that government's sovereignty. For US courts to sit in judgment on foreign firms for their commercial relations with a third country is a challenge to sovereignty of the firms' home countries as well. But Title III expressly prohibits US courts from entertaining the 'act of state' doctrine as a defence in trafficking cases.

From the law's inception, US allies have denounced Title III's extraterritorial reach as illegal interference in their commerce with Cuba¹⁷. Anticipating that their companies in Cuba would become targets of Title III litigation, the European Union filed a complaint¹⁸ against the United States with the World Trade Organization in 1996 and adopted a statute prohibiting EU members and their companies from complying with Title III. Mexico, Canada¹⁹ and the United Kingdom²⁰ passed similar legislation.

In response, President Bill Clinton suspended²¹ Title III for six months, which the law allowed, and in 1998 he signed an agreement with the EU that European companies would not be targeted. In return, the EU agreed not to pursue the WTO complaint. By activating Title III, President Trump has unilaterally abrogated the agreement with the EU and reignited allied opposition. The EU has promised reciprocal measures²² if US claimants try to haul European companies into US courts.

US businesses are not exempt. A Cuban American family in Miami claims²³ to have owned the land on which José Martí International Airport was built, so any US carrier using the airfield could conceivably be sued under Title III. Another family that claims portions of the port of Havana and the port of Santiago has already filed suits against Carnival Cruise Line²⁴ for docking there.

Although only a handful of suits have been filed so far, Title III could damage Cuba's efforts to attract foreign investment. Since virtually all property in pre-revolutionary Cuba was privately held, it will be difficult for a US or foreign company to know in



advance whether a proposed business opportunity in Cuba might become the subject of Title III litigation. Once the suits have been filed, there is no way to undo them, so the tangle of litigation could take years to unwind. Faced with that risk, most US and foreign firms will likely hesitate to enter²⁵ into commercial relations with Cuba. That is a major purpose of Title III – to deter foreign investment and cripple Cuba's economic development.

Limiting travel and remittances

The other elements of the Trump administration's sanctions campaign are the new regulations on travel and family remittances. National Security Advisor Bolton previewed the new Cuba sanctions²⁶ in Miami on 17 April, the same day that Pompeo announced the activation of Title III. Speaking to an audience of Cuban American Bay of

Pigs veterans, Bolton promised to end educational travel, which he denounced as 'veiled tourism', and signaled new limits on the remittances

A Cuban American family that claims portions of the port of Havana and the port of Santiago has already filed suits against Carnival Cruise Line²⁴ for docking there.

Cuban Americans send to family on the island.

Remittances, which were unlimited under President Barack Obama, will be limited to \$1,000²⁷ per recipient

household every quarter – enough to supplement a family's meagre state salary, but not enough to start and sustain a business. The new limits will hit Cuba's nascent private sector hardest because funds from the United States have been the start-up capital²⁸ for many small businesses.

The biggest impact, however, is on travel. As of 5 June, the Trump administration eliminated the people-to-people category²⁹ of educational travel which covered educational and cultural tours run by organisations like National Geographic, the National Trust for Historic Preservation, and the Smithsonian. Authorised originally by President Bill Clinton in the 1990s, people-to-people travel was eliminated by President George W. Bush in 2003, in response to complaints from conservative Cuban Americans in South Florida. President Obama restored it in 2011. Trump, like Bush before him, is pandering to the Cuban American Republican base in Miami in the run-up to the next presidential election.

Last year, 638,000 US residents³⁰ who were not Cuban Americans travelled to Cuba. The vast majority – at least two-thirds if not more – went under a people-to-people licence, and most of them came on cruises. In addition to ending people-to-people travel, Trump also banned all US passenger vessels from visiting Cuba, including cruise ships.

Although the number of US visitors has increased dramatically since 2014, they were less than 15%³¹ of the total foreign visitors to Cuba in 2018, so the reduction in their numbers will be economically painful, but not crippling. The new travel ban will cost Cuba upwards of \$300 million dollars annually in lost revenue. Here, too, the Cuban private sector will suffer disproportionately. US travellers arriving by air are more likely to stay in Airbnb rentals and eat at private restaurants than the Canadians and Europeans who come on tourist vacation packages and stay at the big hotels on the beach. Trump's first restriction on people-to-people travel in 2017, banning individuals from designing their own people-to-people trips, caused a 44% slump³² in private B&B occupancy and a 40% drop in income. The new restrictions will wipe out many of them.

Cubans are not the only ones who will bear the cost of Trump's travel

Links and notes

- <https://www.miamiherald.com/news/donald-trump-says-cuban-voters-love-him-but-hes-wrong-9146019>
- <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-policy-united-states-towards-cuba/>
- <https://www.miamiherald.com/news/politics-government/article156337719.html>
- <https://www.newyorker.com/magazine/2018/11/19/the-mystery-of-the-havana-syndrome>
- <https://www.propublica.org/article/the-strange-case-of-american-diplomats-in-cuba-as-the-mystery-deepens-so-o-divisions-in-washington>
- <https://www.miamiherald.com/news/nation-world/world/americas/cuba/article223567790.html>
- <https://www.miamiherald.com/news/nation-world/world/americas/cuba/article203114054.html>
- <https://www.miamiherald.com/news/nation-world/world/americas/cuba/article219849305.html>
- <https://www.propublica.org/article/john-bolton-national-security-adviser-intelligence>
- <https://www.whitehouse.gov/briefings-statements/remarks-national-security-adviser-ambassador-john-r-bolton-administrations-policies-latin-america/>
- <https://account.miamiherald.com/paywall/stop?resume=228301399>
- <https://www.nytimes.com/2019/04/05/us/politics/trump-sanctions-venezuela-cuba.html>
- <https://www.reuters.com/article/us-venezuela-cuba-economy/investors-in-cuba-wary-of-impact-from-u-s-threats-venezuela-crisis-idUSKCN1PW2UJ>
- <https://www.reuters.com/article/us-venezuela-cuba-oil/venezuela-resumes-domestic-crude-exports-to-cuba-documents-idUSKCN1LT309>
- https://www.huffpost.com/entry/will-trump-open-a-pandoras-box-of-litigation-over_b_5963b584e4b09be68c005468?guccounter=1
- <https://www.brookings.edu/wp-content/uploads/2016/07/Reconciling-US-Property-Claims-in-Cuba-Feinberg.pdf>
- <https://fas.org/sgp/crs/row/R44822.pdf>
- [helms-burton-libertad-act-by-the-united-states/](https://www.consilium.europa.eu/en/press/press-releases/2019/05/02/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-full-activation-of-the-

</div>
<div data-bbox=)

- <https://www.wsj.com/articles/SB931464187753635502>

- <https://www.nytimes.com/1996/06/13/world/canada-and-mexico-join-to-oppose-us-law-on-cuba.html>

- <http://www.legislation.gov.uk/uksi/1996/3171/contents/made>

- <https://www.nytimes.com/1998/04/21/world/european-s-drop-lawsuit-contesting-cuba-trade-act.html>

- <https://www.reuters.com/article/us-eu-usa-cuba/eu-warns-u-s-against-exposing-eu-firms-in-cuba-idUSKCN1RT147>

- <https://observer.com/2019/04/european-union-threatens-us-lawsuit-cuba-sanctions/>

- <http://www.tampabay.com/news/politics/national/trump-faces-decision-on-letting-americans-sue-over-cuba-property/2304815>

- <https://www.claimsjournal.com/news/international/2019/06/03/291230.htm>

- <https://money.usnews.com/investing/news/articles/2019-02-07/investors-in-cuba-wary-of-impact-from-us-threats-venezuela-crisis>

- <https://www.reuters.com/article/venezuela-politics-bolton/trump-security-adviser-bolton-unveils-new-us-sanctions-to-pressure-cuba-idUSW1N20100M>

- <https://www.apnews.com/b2787dedd34345f798b89201fb4d1972>

- <https://money.cnn.com/2014/12/17/news/economy/cuba-remittances/index.html>

- <https://www.apnews.com/67c721daee8143d4a2e6ee8c401bf215>

- <https://www.miamiherald.com/news/nation-world/world/americas/cuba/article226206935.html>

- <https://www.apnews.com/3fe98af293ce4cbd8c60b072054bcf89>

- <https://www.apnews.com/3fe98af293ce4cbd8c60b072054bcf89>

- <https://thehill.com/policy/transportation/335714-trump-weighs-shift-on-cuba>

- <https://www.law.cornell.edu/supremecourt/text/357/116>

- <https://piie.com/bookstore/economic-sanctions-reconsidered-3rd-edition-paper>

policy. In 2017, Engage Cuba, a coalition of business groups, released an analysis³³ concluding that US visitors to Cuba generated \$1.65 billion in revenue annually for US businesses and accounted for more than 12,000 US jobs in the hospitality sector, most of which would be lost if Trump cut off travel. But most importantly, the new restrictions deprive most US citizens of their constitutional right to travel, a right affirmed by the Supreme Court in 1958 in *Kent v Dulles*,³⁴ limited only in cases of dire threats national security.

Trump’s economic sanctions will make life tougher for ordinary Cubans, but they are not likely to bring down the regime, which has survived the US embargo for half a century. The long history of sanctions³⁵ shows that they are effective only when they are multilateral and seek limited concessions. US economic sanctions against Cuba have never met these conditions.

Economic hardship and US hostility will heighten the Cuban leadership’s sense of being under siege, making them less likely to reform the economy

or allow any expansion of free expression. The economic, professional, educational, and cultural ties between people in the United

Trump’s economic sanctions will make life tougher for ordinary Cubans, but they are not likely to bring down the regime, which has survived the US embargo for half a century.

States and their counterparts in Cuba will be harder to sustain. US travel companies will lose access to one of the biggest and fastest-growing tourism markets in the Caribbean.

In the near term, nothing Cuba can do will lead to a relaxation of sanctions because the US goal is regime change and the principal driver of the policy is domestic politics in south Florida. But

hostility to Cuba no longer has bipartisan support. President Obama showed that a policy of engagement and a gradual reduction of sanctions served US interests and was widely popular in the United States, in Cuba, and around the world. If the White House changes hands in 2021, the new president is likely to strip away most of the sanctions President Trump has imposed, resuming the policy of engagement where Obama left off.

William M. LeoGrande is Professor of Government at American University in Washington, DC, and co-author with Peter Kornbluh of Back Channel to Cuba: The Hidden History of Negotiations between Washington and Havana (University of North Carolina Press, 2015).

Bartlett’s Annotated ITAR (“The BITAR”)

The only annotated version of the International Traffic in Arms Regulations

The BITAR provides access to the latest ITAR text and guidance that you need to ensure your organization remains compliant

Find Out More About the Benefits of the BITAR at www.fullcirclecompliance.eu

European Council issues negotiating mandate for recast Dual-Use Regulation



What does the recently issued European Council Mandate say about the shape of EU dual-use controls to come, ask Jasper Helder, Chiara Klau, Daniel Lund and Isabel Foster.

EU Member States are obligated under international commitments to have national controls in place to preclude the proliferation of nuclear, chemical, or biological weapons and their means of delivery. This includes controls over dual-use items, as well as related materials, equipment, and technology for export. In 2000, the EU therefore adopted Council Regulation (EC) No 1334/2000, which created a substantive legislative framework for the control of dual-use items, applicable throughout the EU. The current EU Dual-Use Regulation recast the same regulation in 2009.

However, owing to changing technological, economic, and geopolitical circumstances, in June 2011 the EU began considering reforms to the EU Dual-Use Regulation with the Commission's publication of a green paper and the holding of a public consultation. Feedback from the consultation included a desire from industry for a wider range of EU general export authorisations ('UGEAs'), as well as for a greater convergence of 'catch-all' controls. There was significant push back against the Commission's suggestion for export controls to be used as a tool to protect and support human rights (referred to as the 'human security' approach). This (and other) preparatory work resulted in the Commission adopting its Proposal in September 2016. The Commission Proposal seeks to recast the EU Dual-Use Regulation with the introduction of both a 'system upgrade' as well as a 'system modernisation' to the existing legislation. Among other elements, the Commission Proposal includes several contentious 'human security' aspects aimed at preventing the abuse of cyber-surveillance technologies by governments with a dubious approach to (and record with) human rights.

Key points

- On 5 June 2019, the European Union ('EU') took a step forward with respect to modernising its existing dual-use legislation under Council Regulation (EC) No 428/2009 (the 'EU Dual-Use Regulation'), with the European Council (the 'Council') issuing its mandate for negotiations with the European Parliament (the 'Council Mandate').
- When compared to the proposal first issued by the European Commission (the 'Commission') in 2016 (the 'Commission Proposal'), the Council Mandate appears to reflect a desire from EU Member States for a more limited update to the EU Dual-Use Regulation. In particular, the Council Mandate seeks to remove the substantive provisions relating to cyber surveillance and human rights, which have proved controversial both with EU decision-makers and in industry.
- The Council will now proceed to negotiate with the European Parliament (the 'Parliament') within the perimeters of its Council Mandate and in accordance with the ordinary legislative procedure, with a view to reaching an agreement.

The Parliament adopted its first report (the 'Report') on the Commission Proposal in November 2017. The Report was positive and called on the Commission to go further by introducing (amongst other things) similar penalties for non-compliance across all Member States. The Report also recommended that the proposed legislation contain provisions to capture the new risks posed by emerging technologies. In January 2018, the Parliament voted in favour of the negotiating position set out in the Report and the starting of inter-institutional negotiations with the Council. On 5 June 2019, the Council

finally issued its own perimeters for negotiating with the Parliament.

Proposed changes

The Council Mandate supports several changes to the existing EU Dual-Use Regulation as envisaged under the Commission Proposal. However, it also either rejects or materially alters a number of the substantive provisions. We set out below some of the key changes proposed under the Council Mandate, as compared to the Commission Proposal.

1. Human Security

The Council Mandate removes the suggested (unilateral) Category 10 to Annex I covering surveillance systems, equipment, and components for Information and Communication Technology. This reflects (at least in part) substantive concerns certain EU Member States have raised with respect to the introduction of unilateral dual-use controls at an EU level. From these discussions, it appears as though the certain Member States would prefer, at first instance, for:

1. national governments to introduce unilateral measures themselves through the existing mechanisms under the EU Dual-Use Regulation relating to human rights concerns (i.e., article 8 of the EU Dual-Use Regulation);
2. the EU to put forward a common position in relation to listing such technologies as part of the Wassenaar Arrangement; and
3. EU restrictive measures on third countries to continue including export restrictions on such items (such as in the EU Venezuela sanctions).

In addition, the Council Mandate removes the 'serious violations of human rights or international law' and

‘acts of terrorism’ from the end use ‘catch all’ provisions that the Commission Proposal wishes to add to the existing ‘catch all’ contained within article 4 to the EU Dual-Use Regulation. The Council Mandate also drops from the definition of ‘dual use items’ the term ‘cyber surveillance technology’. By explicitly including the term ‘cyber surveillance technology’ in the definition of ‘dual use item’, the Commission Proposal would see any such item, if not included in Annex I, be covered by the aforementioned end use catch all controls.

2. EU licensing architecture

The Commission Proposal introduces four new UGEAs to help further facilitate trade while ensuring a sufficient level of security through robust control measures (e.g., through registration, notification and reporting, and auditing). The four UGEAs are (i) ‘Low Value Shipments’; (ii) ‘Intra-company Transmission of Software and Technology’; (iii) ‘Encryption’; and (iv) ‘Other Dual Use Items’.

The Council Mandate proposes to drop the UGEAs for ‘Low Value Shipments’ and ‘Other Dual Use Items’. Moreover, the Council Mandate seeks to introduce tighter licensing conditions with respect to the Encryption UGEA. It also reduces the number of permitted countries under the ‘Intra-company’ UGEA, and maintains that users must put in place an internal compliance programme as a condition of use.

The Council Mandate keeps the concept of a ‘Large Project Authorisation’ (‘LPA’). The Council Mandate states that an LPA could be either a global or an individual licence (the Commission Proposal only suggests an LPA as being a ‘global’ licence). Member State authorities would be able to grant an LPA to one specific exporter, in respect of a type or category of dual-use items, which may be valid for exports to one, or more specified end-users in one or more specified third countries. The Commission Proposal suggests that the project duration should exceed one year, whereas the Council Mandate is silent on a minimum length but places an upper limit of four years (unless there is a circumstantial justification for a longer period). Finally, neither the Council Mandate nor the Commission Proposal offer a definition of ‘Large Project’, and so Member States would



likely be left to determine its scope (the Commission has previously put forward the construction of a nuclear power plant as an example).

3. Circumvention clause

To counter illicit trafficking and bring the EU Dual-Use Regulation in line with other EU trade security instruments (e.g., EU restrictive measures), the Commission Proposal introduces a circumvention clause. The clause creates a prohibition on knowingly and intentionally

Both the Commission Proposal and the Council Mandate agree on defining ‘technical assistance’ separately from the definition of ‘technology’.

participating in activities the object or effect of which is to circumvent the: (i) export licence requirement for Annex I items; and (ii) catch all controls for non-Annex I items in respect of export, brokering services, transit, and technical assistance. The Council Mandate removes this clause in its entirety.

4. Technical assistance

Under the EU Dual-Use Regulation, ‘technical assistance’ is an aspect of the defined term ‘technology’ and thus controlled when captured by an export control classification number (‘ECCN’). Both the Commission Proposal and the Council Mandate agree on defining ‘technical assistance’ separately from the definition of ‘technology’.

The Council Mandate also maintains the new definition of ‘supplier of technical assistance’, which would cover: (i) any natural or legal person or partnership resident or

established in a Member State of the EU; (ii) a legal person or partnership owned or controlled by such person; or (iii) another person which supplies technical assistance from the EU into the territory of a third country.

Taken together, both the Commission Proposal and the Council Mandate agree that an authorisation should be required where ‘technical assistance’ relates to dual-use items or their provision, manufacture, maintenance or use, and the ‘supplier of technical assistance’ is aware that assistance is for, or told by authorities that assistance is or may be for, a prohibited end use. That said, the Commission Proposal includes ‘serious violations of human rights or international law’ and ‘acts of terrorism’ as prohibited end uses. However, the Council Mandate removes both inclusions such that it will only apply where the ‘technical assistance’ is for: (i) weapons of mass destruction end use; (ii) military end use in an arms embargoed country; or (iii) use as parts or components of military items exported without licence or in violation thereof.

5. Other points to note

Enforcement mechanism

The Commission Proposal and the Council Mandate align on the need to introduce provisions to support information exchange and cooperation on enforcement between Member States, in particular with the setting up of an ‘enforcement coordination mechanism’ under the Dual-Use Coordination Group. Both, however, stop short of introducing concrete measures to promote the harmonisation of enforcement and monitoring of export controls compliance.

Exporter definition

The Commission Proposal and the Council Mandate extend the concept of ‘exporter’ to include reference to ‘any natural person carrying the goods to be exported where these goods are contained in the person’s personal baggage’.

Licensing for exporters based outside of the EU

The Commission Proposal states that where an exporter is not resident or established within the EU, then the Member State authority responsible

for issuing authorisations is the one where the dual-use items are located. The Commission Proposal indicates that both global and individual licences should be available in such instances. The Council Mandate, however, restricts this provision to individual authorisations only.

Broker definition

The Commission Proposal extends the concept of broker to non-EU companies, which are owned or controlled by an EU resident, or an EU company, as well as to persons carrying out brokering services from the EU into the territory of a third country. The Council Mandate removes this suggestion.

Due diligence

The Commission Proposal and subsequent amendments by the Parliament requires exporters to implement a due diligence process to confirm the absence of any circumstances triggering ‘catch all’ end-use controls (including serious violations of human rights and acts of terrorism). The Council Mandate removes this requirement.

Union general transfer authorisation

The Commission Proposal seeks to introduce a Union general transfer authorisation, which would permit (subject to conditions) the intra-EU transfer of Annex IV items. The Council Mandate appears to remove this concept in its entirety.

Public security includes ‘acts of terrorism’ under Article 8

The Council Mandate explicitly



confirms that Member States may prohibit or impose an authorisation requirement on dual-use items not listed in Annex I for public security reasons, which includes ‘the prevention of acts of terrorism’. This is an addition to the existing wording under Article 8 of the EU Dual-Use Regulation and appears to reflect the Council’s desire for Member States to be more proactive in the use of national lists where appropriate.

Next steps

Taken as a whole, the Council Mandate reflects the Member States’ wish to implement a more modest update to the EU Dual-Use Regulation, as compared to both the Commission Proposal and the documented wishes of the previous European Parliament. At this point, it is difficult to say whether the new incoming Parliament will be receptive to the Council’s watered-down approach, or if it will stick to its previous position. If, however, distance remains between both the Council and Parliament, then it is difficult to see the EU adopting any recast to the EU Dual-Use Regulation in the near future.

As a wider point, the Council Mandate reveals a reluctance on the part of Member States to introduce new measures at an EU level to tackle the perceived risks from emerging technologies through export controls. The Parliament made the introduction of such measures a key recommendation in its November 2017 Report, and may well continue to raise the issue in the forthcoming negotiations with the Council. Whilst there are existing mechanisms in place for Member States to introduce unilateral controls, any national government contemplating any such measures would likely face considerable pressure from industry to desist. It therefore raises the question, especially in light of recent developments in the United States and elsewhere, as to how the EU will seek to address similar concerns across Europe regarding the control of emerging technologies (if not through the EU Dual-Use Regulation).

Partner Jasper Helder, senior counsel Chiara Klau, and associates Daniel Lund and Isabel Foster are in the International Trade practice at Akin Gump in London.

jasper.helder@akingump.com
chiara.klaur@akingump.com
daniel.lund@akingump.com
isabel.foster@akingump.com



The CFIUS Book

A guide on how to navigate an investment or acquisition in sensitive industries or companies in the United States.

English and Chinese versions available
www.worldecr.com/books



China already implementing new export control law in response to Huawei restrictions



Recent pronouncements by the Chinese government suggest a fast-tracking for the introduction of its new export control law, write Tim Hesselink, Marc Padberg, Eline Mooring and Ton Bendermacher.

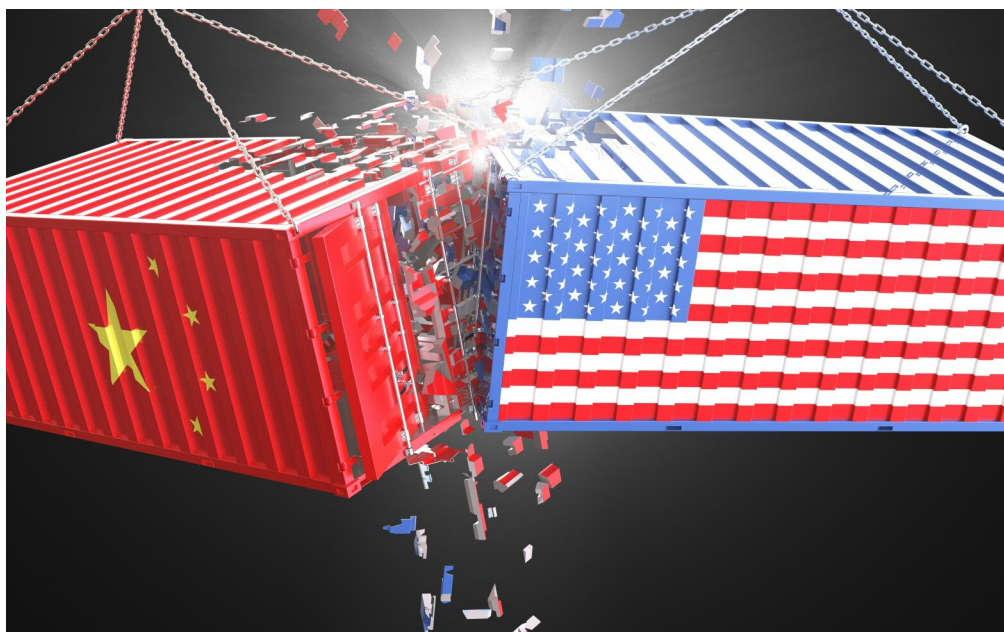
China has recently announced that it will establish a mechanism to control exports to the United States, reportedly to forestall and prevent national security risks. This announcement follows the listing of Chinese telecoms company Huawei on the US Department of Commerce Entity List, in response to which China has threatened to punish foreign companies that cut off ties with Huawei by listing them on an 'Unreliable Entities List'. This mechanism, developed by the Chinese National Development and Reform Commission ('NDRC') pursuant to China's National Security Law, makes it possible to control the export of sensitive technology and rare earth metals required to produce items such as smartphones, lasers, satellites and hybrid and electric cars. This export control mechanism seems to clearly link to the draft Chinese Export Control Law ('ECL'), first proposed by the Ministry of Commerce ('MOFCOM') in 2017. The US-led Huawei restrictions may result in a faster implementation of the ECL.

This article recaps and reviews the draft legislation in order to find out what one can expect from China's new ECL in the near future.

Reform of the current regime

China's current export control framework is made up of a patchwork of various laws (such as the Customs Law, Foreign Trade Law, and Criminal Law) and administrative rules and regulations (e.g., the Regulations on the Import and Export Control of Technologies 2011), which were last amended more than a decade ago.

China's legal framework for export control is relatively young, originating in the 1990s. Unlike the EU Member



States and the US, who joined the international export control regimes a long time ago, China is not a member of the Wassenaar Arrangement, the Australia Group, the Missile Technology Control Regime, nor the Nuclear Suppliers Group.

For a good understanding of China's export control regime, it is important to remember that, for trade purposes, Hong Kong, Taiwan and Macau are considered foreign territory. The transfer of goods from mainland China to these areas is thus considered an export. This means that if the exported goods are controlled items – i.e., the items are subject to export control – compliance with the export control legislation is required in addition to, for example, the customs legislation.

Export Control Law

In June 2017, MOFCOM released a draft ECL, which is aimed at upgrading

the country's existing regime consisting of various laws and regulations. The new ECL involves a number of far-reaching changes. MOFCOM will be responsible for the export control regime, under the supervision of the State Council and the Central Military Commission. MOFCOM's subordinate division, the Bureau of Industry, Security and Import and Export Control will be responsible for reviewing and granting export licences, conducting investigations and enforcement. The Chinese customs authorities act as the gatekeeper of the physical export. What remains similar to the current regime is that the export of military items is exclusively allowed for state-authorized trading companies and dual-use items can only be exported by companies in possession of an export control licence.

New is the expansion of the definition of export: not just the

transfer of controlled items to places outside mainland China, but also the exchange of items between Chinese companies and non-Chinese companies within mainland China is captured under the draft ECL. For example, the sale of a dual-use item from a Chinese technology company to an EU company operating in China is subject to export control. With that, the draft law introduces the term ‘deemed transfer’, which appears to be similar to the concept of ‘deemed export’ in the US, being the transfer of controlled technology to a foreign person in the US for which an export control licence is required.

In addition, China is introducing the concept of ‘re-export’, which is again similar to the US regime and is likely to expand the extraterritorial scope of the Chinese export control legislation. According to this concept, a foreign-manufactured item can be subject to Chinese export control if the content of that item is of controlled Chinese origin. Although the draft law does not provide further details on the term ‘re-export’, it is expected that China – like the US – will apply a 10% *de-minimis* rule. In short: the foreign-manufactured product in question is only subject to export control if the content of controlled Chinese origin does not exceed a 10% threshold.

To conclude, while the Chinese customs law treats warehouses and bonded zones as outside of China’s customs territory, the ECL expands the definition of export to include transfers from these areas.

Control lists

The draft ECL introduces four categories of controlled items: dual-use items, military items, nuclear items and other goods, technologies and services that are related to national security. Not only tangible goods, such as materials and equipment, are subject to the export control legislation, but also intangible goods, such as technology and services (e.g., export in the context of research and product development). The current separate lists of controlled items (such as the individual lists for nuclear export control, biological dual-use items, precursor chemicals etc.) will almost certainly be consolidated into one list of military and dual-use items. The export of nuclear items will remain to be arranged separately and will therefore not be included in the

consolidated list. Unfortunately, the draft text contains no further information about the aforementioned consolidation plans. However, the draft

The draft law provides for the possibility of initiating retaliatory measures against countries which have subjected China to discriminatory export control measures.

text does mention that items outside the control lists could also be controlled upon approval of the State Council, the Central Military Commission and their designated authorities, for a maximum of two years. In addition, the draft text contains a so-called ‘catch-all provision’, with which the Chinese authorities have the ability to extend the control to items not included in the control list, on a case-by-case basis for national security reasons.

China’s enforcement policy and export control ‘retaliation’

The draft law provides MOFCOM and the executive authorities with further investigative and enforcement powers. This includes, for example, the authority to enter and check business premises, conduct interviews, seal and seize assets, and freeze bank accounts. In addition, the new law prohibits any violation or circumvention of export controls. In this context, the ECL mentions exporting without a licence, withholding information or providing false information or materials, obtaining a licence by fraud, bribery or through other illegal means and the avoidance of checks related to export control as punishable conducts. Also, the delivery of controlled items to organisations and persons that are subjected to sanctions is prohibited. It is therefore advisable for companies with supply chains in China to set up strict screening procedures. Violations of the ECL can result in high fines for both companies and individuals – up to 10 times the yearly business revenue or a fine up to RMB 500,000, (approximately EUR 64,000) for companies; and RMB 300,000, (approximately EUR 38,000) for personal liability. Moreover, serious reputational damage must also be taken

into account as the draft law introduces a public register which is maintained by the Chinese authorities which lists non-compliant entities. On the basis of this list, the Chinese authorities have the power to prohibit the export of controlled items to such listed entities. Lastly, the draft law provides for the possibility of initiating retaliatory measures against countries which have subjected China to discriminatory export control measures.

Final remarks

It is clear that with the recent announcement to establish a mechanism that could control the export of rare earth metals to the US, China is taking serious action. Rare earth metals are crucial to the tech and defence industries and China accounts for more than 90% of the global production and supply of these materials during the past decade. This puts China in a powerful position. US defence manufacturers and companies that adopt discriminatory measures such as cutting supplies to Chinese entities like Huawei, are likely to be among the first entities that will face restrictions on importing China’s rare earth metals. While there is still no specific information about the implementation timeline for the ECL, the recent developments show that export control is high on China’s priorities list. With the US-led restrictions on telecoms company Huawei, it seems that China is anticipating the implementation of its new ECL. Since more information about the to-be-established mechanism is yet to come, the impact of the consequences have still to be seen in practice. For now, it is important for companies doing business in China to monitor the developments and prepare for possible export control restrictions.

Tim Hesselink, Marc Padberg and Eline Mooring are attorneys and Ton Bendermacher is of counsel at Kneppelhout & Korthals N.V. in Rotterdam, The Netherlands.

th@kneppelhout.nl
mpd@kneppelhout.nl
em@kneppelhout.nl
tb@kneppelhout.nl

Thailand to start enforcement of export controls in 2020



Incoming legislation puts Thailand in place to implement its obligations under UNSCR 1540, write Stuart Simons and Sujitra Sukpanich.

The Trade Controls on Weapons of Mass Destruction (‘TCWMD’) Act, Thailand’s export control regulation on dual-use and military items, received Royal assent and was published in the *Royal Gazette* on 30 April 2019. The act will become effective on 1 January 2020 and is Thailand’s implementation of its international obligations under the United Nation’s Security Council Resolution 1540 to counter the global proliferation of weapons of mass destruction (‘WMD’).

The TCWMD Act places upon Thai Customs the task to control the export of goods that can be used for military ends or in the production process of weapons. The aim of the act is to prevent the goods from being acquired by sanctioned entities and/or used for the production of WMD abroad.

Control lists coming

The specific goods that will be subject to the control measures depend on the goods lists, which are still under consideration by the Department of Foreign Trade (‘DFT’). What has been announced so far is that there will be three lists: a list with dual-use items (items with both a civil and military purpose); a list with military goods; and a self-certification list. These lists are expected to be published in the near future and before the entry into force of the act at the beginning of next year.

In the first two lists, goods are classified with export control classification numbers (‘ECCN’) in accordance with international agreements and the US and EU export control regimes. Exporters of these goods will have to request a licence from specified government authorities prior to shipping out and provide the reasons for export. Attempts to export in-scope goods without a licence will

lead to blocked shipments at the border and penalties.

The self-certification list contains HS codes (customs tariff codes) that are also used in the traditional customs declaration process of goods during

The specific goods that will be subject to the control measures depend on the goods lists.

import and export. Exporters of goods with HS codes that match the HS codes in the list will have to self-certify the non-violent end use of their products abroad. While self-certification can be considered as less burdensome, exporters still have to be able to support their assessment with evidence in case of Customs audits or queries.

Exporters will be able to know whether their products fall under any of the designated lists by making use of an online government assessment tool (e-TCWMD). The tool can already be tested, but is still subject to changes. Through the application of a detailed questionnaire and based on the exporter’s answers, the tool determines whether a product is subject to control measures (dual-use item or military good). In addition, exporters can also fill out the HS code of their product and the tool will confirm whether this HS code is included in the self-certification list. In its final form, the tool will contain a platform for online licence application or self-certification.

Even though the final lists have not yet been announced, the DFT has already published some indicative lists with dual-use items and HS codes. The scope of products in the dual-use items list is very similar to the EU Dual-Use Regulation goods list.

In anticipation of the release of the definitive goods lists, exporting companies should start assessing their goods to determine risk categories and develop standard operating procedures for the goods identification and licence application process to prevent any disruption of their supply chain. Employees that handle in-scope products or those that are involved in the export process have to receive training to become acquainted with this new aspect of their job.

There will be two types of licence: transactional licences and bulk licences (which are licences that apply for a longer period). Only companies with a qualified internal compliance programme (‘ICP’) that adequately self-screens and monitors trade transactions will be able to apply for the bulk licence.

Screening for bad actors

Apart from self-certification and export licence requirements, the TCWMD Act also contains a catch-all provision which allows Customs to block the export of any shipments it considers suspect. Exporters are therefore expected to screen their foreign business partners against sanctioned party lists and must produce trustworthy information about the activities of the foreign buyers and end use of the product, especially in destination markets that are considered high-risk zones. Such comprehensive due diligence measures will allow the exporter to convince the authorities that their exports pose no danger or harm.

The act will be enforced by means of civil, criminal and administrative penalties, against exporters who fail to comply with its provisions.

Stuart Simons and Sujitra Sukpanich are in the Global Trade Advisory team at Deloitte Thailand.

ssimons@deloitte.com

ssukpanich@deloitte.com

INDUSTRY PRACTITIONER
MASTERCLASS

**PRACTICAL INSIGHTS TO
DEVELOPING AN EFFECTIVE INTERNAL
COMPLIANCE PROGRAM IN ASIA FOR
STRATEGIC TRADE MANAGEMENT**

WHO SHOULD ATTEND?

For executives and professionals who are responsible for export control or strategic trade management compliance across Asia within their companies and/or tasked to develop an internal compliance program (ICP). Participants should ideally have a basic understanding of the broad principles of strategic trade controls prior to attending this course.

COURSE DETAILS

Date : 21st - 22nd August 2019

Time : 9AM - 5PM

Venue : Suntec City Convention Centre

Public: S\$1600

Clients and Alliance Partners: S\$1300

CAPTICIS Members: S\$900

Fee includes lunches and tea breaks across the 2-day course duration and a Proficiency Test at the end of course with certification by the Centre of Asia Pacific Trade Compliance & Information Security (CAPTICIS)

SELECTED HIGHLIGHTS OF THE COURSE

- Overview of the essential aspects of the key national strategic trade control regimes and internal compliance program requirements in Asia
- Dealing with the extra-territorial reach of the US and Japan within your business in Asia
- Walkthrough of business considerations when customising and managing your internal compliance program
- Practical application of strategic trade controls in businesses and industry best practices
- Monitoring of ICP effectiveness levels and know-hows to conduct an export control internal audits and manage non-compliance incidents
- Sharing of actual case studies of ICP development and implementation journeys in Asia

**Note that the above outline may be subject to changes.*

For more information, please scan QR code or email to angelia@actradeadvisory.com or eugene@actradeadvisory.com



OUR TRAINERS

Our Trainers are highly experienced export control and trade compliance industry practitioners and advisors with rich experiences in developing and managing internal compliance programs, especially in Asia.



ANGELIA CHEW
Founder & Managing Partner
of AC Trade Advisory



EUGENE JANG
Co-Founder & Partner
of AC Trade Advisory



GEORGE TAN
Principal of Global Trade
Security Consulting (GTSC)

Knowledge Partner and Organiser:



In collaboration with:



Supported by:



Utilising identity access management solutions to safeguard sensitive data



Export compliance professionals understand the importance of controlling physical access to certain areas and items. IAM solutions offer a way to manage variable access rights and control access to technology and data. Steven Brotherton and Amie Ahanchian describe the benefits of IAM for export compliance.

In today's business world, data can be both the driver of success and the cause of significant exposure for an organisation that experiences a data breach. In this article, the Global Export Controls and Sanctions Practice of KPMG LLP examines data access and protection by leveraging identity access management ('IAM') solutions and how those solutions can keep you ahead of the curve when it comes to data protection.

The IAM framework and maintaining effective control

As an export control officer, do you know where your company's data is stored? More importantly, are you familiar with how your data may be accessed? The world today provides instant access to infinite amounts of information, be it via a cloud-based service, or the phone you hold in your hand. Never has it been more important from a business perspective to control how your data is maintained, and furthermore accessed.

IAM solutions create a framework for data access by establishing roles and restrictions for various users based on their specific data needs. Specifically, IAM is based on various accounts and digital identities associated with those accounts to establish security parameters around your sensitive business data and controlled technology, ultimately allowing the right people to have the right access to the information required for their specific job function. Failure to create these parameters ultimately opens the door to a host of potentially irreparable damages, including not only loss of sensitive data information for criminal activities and insider threats, but export control violations as well.

It is likely that your company already employs some type of IAM

component to restrict access to sensitive or proprietary data. For example, your payroll department has access to personnel records that an

The need for IAM hits home when it comes to protecting controlled technology from unauthorised persons.

engineer would not need access to and, conversely, payroll would not need access to export-controlled technical data. Even further, an engineer working on one product may not need access to technical data on unrelated product lines, and IAM can be used to tailor an individual's access to only those areas of need. For the export control professional, taking a proactive approach to managing these access

rights will assist in mitigation of inadvertent or deliberate attempts to view or obtain controlled data.

The intersection of IAM and export compliance

The need for IAM hits home when it comes to protecting controlled technology from unauthorised persons, including but not limited to certain employees, foreign and domestic visitors, and external business partners. The US government maintains stringent regulations that govern the export of controlled technical data or technology, namely the International Traffic in Arms Regulations ('ITAR') and the Export Administration Regulations ('EAR'), and non-compliance with these regulations can be damaging.

As a comparative example, imagine the distinct levels of physical access that employees working with defence articles in a facility governed by the



Typical data access levels for departmental functions

Publicly available	Proprietary	Regulatory Controlled	Classified
Publicly available information is generally accessed without limitation and available to all personnel across the entity	Proprietary information is generally limited to those that need access to support their job function, such as Human Resources	This level of data access should be restricted to export professionals responsible for compliance with various government regulations	The highest levels of data security are applied to employees that are cleared for access by the US government

ITAR may possess based on their role within the organisation, their job function, and their level of authorisation:

- Some professionals may only have access to the office space and conference rooms;
- Other employees, who work on the assembly line, may only require access to the manufacturing floor; and
- Select authorised personnel only may access the ITAR-restricted areas with controlled information.

At a facility, monitoring access to physical areas and products is fairly straightforward and achievable through the use of physical security protocols (e.g., locked doors, electronic access cards, cameras, signage), implemented ITAR procedures, and training.

Considering the fallout that would be caused by unauthorised exports or release of controlled data, it is of critical importance to design and maintain an IAM solution that implements user-verification gates at strategic checkpoints to establish proper role accounts, thereby protecting against any unauthorised releases. By first evaluating a user's credentials, the regulatory requirements and the company's business needs prior to provisioning any access, export compliance professionals can take their time to work with information technology ('IT') teams and set up the appropriate network profile. Once established, the company can have greater confidence that there are sufficient electronic controls in place to protect sensitive data from those that may not be authorised.

The graphic above provides an example of the level of access that a particular function may require.

Understanding sensitive and controlled data

The stakes for data loss increase when dealing with sensitive or controlled data, which is commonly understood as information that must be protected against unwarranted disclosure. Controlling access to sensitive data is necessary for a myriad of legal and ethical reasons, including control of proprietary and private data, and, in the US, for example, compliance with regulations such as the ITAR and EAR.

Technical data can have varying levels of control that will dictate specific limitations on who may have access to it as well as how it may be disseminated. Specifically, the release, or export of technical data or controlled technology may require a licence or

Technical data can have varying levels of control that will dictate specific limitations on who may have access to it as well as how it may be disseminated.

other government authorisation depending on the end-user and ultimate end use or application of the data.

Exports of controlled technical data or technology can occur via many means, including email, oral communication or visual inspection and can occur both internationally, or within the United States. The latter, known as a 'deemed export', highlights the importance of knowing who you are dealing with when discussing or handling controlled data, because once the data has been released or discussed, the export has occurred.

All of this points to the importance of the export control professional

maintaining an active presence in the ever-changing landscape of data protection. Given the regularity of technological advancement and the consistent updates to regulatory requirements, it is extremely important for the international trade practitioner to work in conjunction with IAM leadership to ensure the most current user rights are considered.

IAM solutions

Determining the level of IAM solutions that is right for your particular business structure is dependent upon a number of factors, including the type of data created or stored, your customer base, government control or classification level, and the requirements set forth by any governing agencies. Simple, process-based solutions exist that are tailorable to organisations of all sizes, and can support cross-functional implementation to allow multiple users from Human Resources, IT, Contracts, Security, etc. Access can be controlled by assigning user rights and entrusting administrative controls within a hierarchy of approvers.

When the make-up of a business requires more stringent protection, IAM solutions are predicated on utilising authoritative sources for users which enable the creation of the user and a process to define user's roles and privileges. In addition, management of the permissions and entitlements as the user moves within the organisation, and updating access rights as roles change, is more likely to be necessary when employing a large number of people and utilising a larger data-management network.

As organisations continue to develop their technologies, utilising multifaceted IAM solutions becomes critical. The use of IAM through biometric restrictions or dual-factor

Some examples of access restrictions

Principle of least privilege

Allow only view access, limiting the user only to view-data rights. Adding, updating, or amending data is not authorised.

Provisional access

User has access to certain operational systems like Windows, but not to development or testing platforms or mainframe systems.

Restricted access

Limiting users to specific roles that can access only certain parts of systems, databases, and information.

Multifactor authentication

Utilising a combination of something the user knows (like a password), something the user has (like a RSA token), and something the user is (like biometrics), to authenticate individuals and grant them access.

authentication is becoming more common as companies navigate the continually changing landscape of information control. Understanding the type of data you are trying to protect and the nuances of IAM will help you determine the best solutions for your company.

There are different ways to implement IAM policies to define and enforce role-based access control models, based on an organisation's specific needs (see above box, 'Some examples of access restrictions').

Whatever solution you deploy, keep in mind that without collaboration between the system administrators and export control practitioners, the

solution may have gaps that give rise to potential violations and subject the company to increased risk and exposure or loss of data.

IAM key benefits

The values to be realised from a successful IAM system implementation are continually increasing. IAM solutions provide assurance that access controls are effectively implemented across your entity, and bring about a host of benefits including enhanced security features, threat-environment monitoring, and operational efficiency. Of paramount importance, maintaining an effective IAM system will allow your organisation to keep pace with ever-changing laws and regulations.

Implementing a well-defined process of identity lifecycle management and access provisioning to applications helps to act as a proactive measure and enables users to have necessary access based on the principles of least privilege, at the same time making the user efficient from the very get-go. It also empowers end-users by simplifying and automating application access requests and fulfilment processes.

A final benefit to IAM solution implementation is the ability to audit and monitor user access. Legal and regulatory requirements continue to stiffen, and periodic review for IAM internal processes and policies will drive a culture of compliance and assist with the identification of gaps in the system. Effective utilisation of data control and management systems allows for the tracking of all activity, including the source of access, user authentication, data removal, and approval activities.

Taking it one step further,

companies may elect to link user-role accounts to physical security controls and/or meeting invites, providing greater assurance that users collaborating in certain buildings, floors, conference rooms, or even the attendees on a meeting invite, are authorised.

While this may seem like a tall order, chances are your company is already leveraging IAM solutions to some degree. With that in mind, export compliance professionals should reach out to IT professionals and explore ways to leverage the company's existing IAM framework to meet the company's export compliance needs.

Conclusion

The risks associated with the loss of sensitive information have become too great to ignore and the majority of companies have become resigned to the eventuality that a data breach is a matter of when, not if. Companies taking aggressive and proactive measures against this possibility, especially with respect to export controls, are subscribing to a smart tactic in mitigating unauthorised exposure to controlled data.

For the export control professional, it is not a matter of instituting a data protection solution from scratch, but enhancing existing systems and leveraging your international trade leadership to get the most out of your company's current IAM capabilities. Accordingly, IAM is a practical and accessible solution to ensure comprehensive controls are in place to protect against unapproved data access.

The authors would like to thank Jenna Glass, senior manager, and Ben Meyer, senior associate, for their contributions to this article.



Would you like to find out more about IAM and other best practice solutions?

Meet Steven and Amie this October at the WorldECR Forum in London and DC.

Download the Forum brochure at worldecr.com/conference-2019/

Steven Brotherton is a principal and leader of the global export controls and sanctions service line and Amie Ahanchian is a managing director, global export controls and sanctions service line, in the Trade & Customs Services practice of KPMG LLP.

sbrotherton@kpmg.com
aahanchian@kpmg.com

A special report from
WorldECR



US SANCTIONS AND ENFORCEMENT



Welcome to this special report from *WorldECR*, the journal of export controls and sanctions.

Why 'US' sanctions particularly? The United States has always imposed sanctions in furtherance of its own foreign policy objectives. President Trump's mercurial regime has bucked the trend, however, of alignment with allies – and the US Congress and its members have their own concerns which are reflected in legislation like CAATSA – the Countering America's Adversaries Through Sanctions Act.

What are the consequences of this heady cocktail of threats and prohibitions? That's something explored in our extended editorial, while our contributors, all recognised leaders in the field of trade compliance, reflect on the specific aspects of a multi-layered legal backdrop to cross-border transactions.

To be forewarned is to be forearmed, they say. While disclaimers apply, we hope that this report provides stimulating reading as we head along the rocky path toward 2020.

*Tom Blass, Editor, WorldECR
July 2019*



CONTENTS

3 NO TIME LIKE THE PRESENT

We speak to leading sanctions lawyers on both sides of the Atlantic about the evolving policy tool that is the imposition of sanctions – and how best to advise clients in an era of change.

24 THE GOING GETS TOUGH

Compliance professionals share their experiences of how different industry sectors are coping with recent sanctions and enforcement developments and offer suggestions on how the challenges can be mitigated.

INSIGHT

20 Recent OFAC policy changes and settlement trends suggest shifting enforcement priorities

By Ryan Fayhee, Roy Liu and Alan Kashdan, **Hughes Hubbard & Reed**

21 Reforming US secondary sanctions: What's wrong that can be righted?

By Kay C. Georgi, Marwa M. Hassoun and Regan K. Alberda, **Arent Fox LLP**

22 Navigating the swamp: staying competitive during a resurgence of export controls

By Jeff Snyder, Michelle Linderman and Dj Wolff, **Crowell & Moring**

23 Trading tariffs for sanctions?

By Barbara D. Linney, **Baker Hostetler**

30 OFAC clarifies its compliance expectations

By Satish M. Kini and David G. Sewell, **Debevoise & Plimpton**

31 Helms-Burton litigation adds a wrinkle to business ventures in Cuba

By Cari N. Stinebower and Christopher B. Monahan, **Winston & Strawn**

32 Four important lessons from recent US export controls and sanctions enforcement actions

By Brian J. Fleming and Timothy P. O'Toole, **Miller & Chevalier**



NO TIME LIKE THE PRESENT

WorldECR speaks to leading sanctions lawyers on both sides of the Atlantic about the evolving policy tool that is the imposition of sanctions – and how best to advise clients in an era of change.

As at the beginning of July 2019, US President Donald Trump is returning from his visit to the demilitarised zone between North and South Korea, where he met his geopolitical frenemy, Kim Jong-un. Meanwhile, the Supreme Leader of Iran, Ayatollah Khamenei, is smarting – or possibly amused by – his recent inclusion on the OFAC Specially

Designated Nationals And Blocked Persons (‘SDN’) List, which may have been a factor in Iran’s decision to exceed agreed uranium enrichment limits under the Joint Comprehensive Plan of Action (‘JCPOA’). The fall of Nicolas Maduro in Venezuela, once touted as inevitable, has yet to happen. President Vladimir Putin of Russia has given a smirking promise not to

interfere in the United States’ 2020 presidential election. And the (now former) UK ambassador to the United States is *persona non grata* in Washington, DC, following the leak of diplomatic cables where he said rather unflattering things about the leader of the nation that hosted him.

‘Not normal is the new normal. Expect the unexpected. They all sound

like clichés but they're true...' is the neat summary of events provided by one of the lawyers we spoke to for this special report.

And at the heart of so much of this international activity and disruption are the sanctions. Sanctions – the ever-attendant geo-financial meta

whom they apply. No one expected 231 tariffs to be applied to Germany, Canada, or Japan. There may be no loyalty to old allegiances,' she adds.

Not all observers find it easy to detect method in that approach. 'The way the Trump administration is using sanctions tools as part of its trade

actions in and over international waters, including the targeting of United States military assets and civilian vessels.'

Given the ayatollah's apparent lack of dollar-denominated holdings and his reputed aversion to travelling outside his own country, the designation is essentially a symbolic gesture. But in an age where the foreign policy scene has reverted to the grandstanding of 'big men', it's certainly potent.

There is perhaps no better example of the gulf (no pun intended) between the United States and many of its traditional allies as regards foreign policy than the post-JCPOA fall-out. In response to the US withdrawal from the deal, and a ratcheting-up of sanctions on Iran, Iran has said it will no longer be bound by the terms of the JCPOA – unless the remaining partners to the plan of action can deliver Iran some concrete benefits.

EU Member States, France, Germany and the United Kingdom have launched a facility designed to facilitate 'legitimate' trade with Iran, INSTEX.

'France, Germany and the United Kingdom informed participants that INSTEX had been made operational and available to all EU Member States and that the first transactions are being processed,' said the EU in a recent press statement, adding, 'Ongoing complementary cooperation with the Iranian corresponding entity (STFI), which has already been established, will speed up. [The founding members] confirmed that some EU Member States were in the process of joining INSTEX as shareholders, the special purpose vehicle aimed at facilitating legitimate

business with Iran. They are also working to open INSTEX to economic operators from third countries.'

Few have great hopes for INSTEX, and the small ones that remain have been largely dashed by Iran's threat to enrich uranium beyond the levels stipulated by the JCPOA unless the remaining parties to the agreement can do something to counter the devastating impact of US sanctions on the Iranian economy.



'The way the Trump administration is using sanctions tools as part of its trade policy makes it very difficult to assess what's going to happen and plan for business.'

Kay Georgi, Arent Fox

commentary on the State of the World – it seems are everywhere.

That ubiquity has a distinctly US feel to it. As Dr. Pascal Ditté of sanctions-intelligence.com points out, between January 2018 and June 2019, the OFAC SDN List grew by 29.3% to a total of 7,725 entries, the list changing 124 times during that period, which equals a list change every 4.4 calendar days on average. Busy times indeed.

Perhaps because of these uncertainties, the fluidity of numerous quasi-connected situations, and the lack of a focal point upon which previously aligned nations may once have converged, sanctions practitioners report a patchwork of concerns from clients, who have to spend increasing resources evaluating numerous exposure risks and the extent to which they may or may not apply.

Is there an underlying pattern in current sanctions and foreign policy, particularly as driven by the White House?

'The consistency lies in the unexpected,' DC-based sanctions lawyer Giovanna Cinelli of Morgan Lewis tells *WorldECR*. 'If you read Trump's writings – like *The Art of the Deal* – you'll see that he's the master of situational awareness and looking for opportunities for leverage. He seeks to use whatever tools are available, and he creates them if they aren't, instead of resolutely clinging to norms.'

All his actions in the trade sphere, she points out, are in line with the 'ground rules' of existing statutory authority.

'Where the surprise tends to come is with the unexpected nature of those to

policy makes it very difficult to assess what's going to happen and plan for business,' says Kay Georgi, head of the International Trade practice at law firm Arent Fox in Washington, DC. As examples of unexpected changes, Georgi cites the apparent reversal or annulment by the president of the Commerce Department's inclusion of Huawei on the Entity List and more recently an apparent second reversal of that decision by Secretary of Commerce Ross. As a result, it's increasingly difficult to forecast the way export controls and sanctions tools are being used almost interchangeably to address national interests.

Gulf of misunderstanding

On 24 June, the United States' Iran sanctions regime, now wholly at odds with the stance of the European Union and other permanent members of the UN Security Council, claimed its most high-profile scalp: that of the Supreme Leader of the Islamic Republic of Iran, the Ayatollah Khamenei. The authority to do so was granted under an executive order that President Trump signed in response to what the EO describes as 'the actions of the Government of Iran and Iranian-backed proxies, particularly those taken to destabilize the Middle East, promote international terrorism, and advance Iran's ballistic missile program, and Iran's irresponsible and provocative



Debevoise
& Plimpton

**“Nothing but
exceptional”**

Our market-leading sanctions compliance and enforcement practice is made up of attorneys with extensive experience from the private sector and in government.

The depth of the practice means we are able to build the right teams for the job at hand. That may be anything from a lean partner-led team to focus on a specific issue, to a bench of heavy-hitters for highly complex, business-critical sanctions matters.

We are consistently recognised by *WorldECR* as a leading practice, with the *WorldECR Awards* quoting “glowing praise from clients, with one noting, ‘consultations are always clear and risk-oriented, with a unique expertise on how sanctions regulation works in different jurisdictions,’ while another hails it as ‘nothing but exceptional’.”

www.debevoise.com

‘Doomed from the outset,’ said one lawyer. ‘No great shakes,’ said another.

In that US companies have long been prohibited from dealing with Iran, the messy situation is one that mostly impacts non-US companies, albeit that they may be subsidiaries of US parents.

Though, even then, the extent of the ‘problem’ is reduced because, as Mattias Hedwall of Baker McKenzie points out, ‘The practical problems are not, in effect, so significant, because companies have just stopped doing commercial business with Iran and of course the banks won’t process transactions. Yes, there are some companies with some dealings, but these are extremely limited, and are dealt with in a very structured way so as to not breach sanctions. As regards the SPV [INSTEX], no bank wants to deal with it, so there’s no way of getting the payments out. So in practical terms, again, it just doesn’t work.’

And yet, there’s an irony in that the purpose of INSTEX is primarily to facilitate the export of ‘AGMED’ products, i.e., the kinds of food and

‘hugely complex triangulation of banking structures’ for the drugs to reach their intended destination.

‘If you look at the US licences for



‘The best things that non-US companies can do right now is make sure that they have contractual provisions in place so that if sanctions are removed or imposed, they can respond appropriately.’

Matt Butter, Addleshaw Goddard

medical supplies permitted to be exported under US sanctions licences.

Kay Georgi notes that she recently spoke at an Italian conference where an audience member described the near-impossibility of exporting oncology medicine from Europe to Iran. Because most banks wouldn’t go near deals involving Iran, it was reportedly necessary to construct a

exporting AGMED, they would preclude end-users with any nexus to the military,’ says Georgi. ‘It just so happens that – as in the United States – there are a number of military hospitals in Iran. So the risk is just too high for most companies, or banks, to take on.’

Such observations could be read as making a compelling argument for the

Huawei and the Entity List – sanctions by another name?

When Chinese technology company Huawei was added to the Department of Commerce’s Entity List, the furore created eclipsed, arguably, even that of ZTE’s inclusion back in 2017. Of a sudden, the world’s business community and media were alerted to the impact that ‘the List’ could have not only on the listed party, but entire and complex supply chains spread across the world. A shift toward the interchangeability of ‘export controls’ and ‘sanctions’ has been incrementally visible for some time. Recent sanctions measures, both EU and US, impose nuanced restrictions on what can be exported and to whom.

The 21 May designation of Huawei, and 68 non-US affiliates, meant that ‘For all of the entities added to the Entity List in this final rule...BIS imposes a license requirement for all items subject to the EAR and a license review policy of presumption of denial. Similarly, no license exceptions are available for exports, reexports, or transfers (in-country) to the persons being added to the Entity List.’

At the same time, Commerce published a temporary general licence (‘TGL’), valid initially for three months, permitting certain exports and transfers to Huawei of certain items for certain purposes. In late June, the US president, attending the G20 summit, announced that ‘American companies can sell their equipment to Huawei’ so long as such sales ‘don’t present a great, national emergency problem.’

WorldECR understands the current status of that intervention to be unclear. But we know that that uncertainty is causing many companies for whom Huawei represents a very major customer, some sleepless nights.

‘The thing that worries me about that incident is that – by effectively sanctioning Huawei – the administration appears to have forgotten the human cost [of those kind of activities]. There are companies that have not only lost contracts, but are being sued, and have essentially furloughed employees, on account of that designation,’ one told WorldECR.

‘The conditions [of Huawei’s inclusion on the Entity List] are narrowly drawn, but the statements that have been made about the situation are very broad. The TGL allows the sale to Huawei of items not controlled for export, but the long and short of it is that many companies are going to have a great deal of difficulty planning for the future.’

The extent to which Huawei’s suppliers and customers continue to engage with it, or decide to cut their losses, will depend on their risk appetite and the nature of their relationship. ‘If it’s huge, they’re going to continue to do the business that they can under US law,’ suggests Kay Georgi of Arent Fox.

‘It does’, she says, ‘illustrate the blurring of distinctions between export controls and sanctions law. This has been happening for some time, with the full support of Congress.’

But, notes Barbara Linney of Baker Hostetler, some companies may be mistakenly conflating the two concepts in their quest for compliance: ‘There seem to be a lot of companies who thought that the listing was akin to an OFAC SDN listing, which may be the result of using third-party software. It really depends on a company’s policy for resolving “hits”. Some take the view that if they get any hit, then the listed party is someone they don’t want to deal with. But you need to do more digging to understand the specific implications of a hit.’

‘A lot of companies can rejigger their supply chains and move production offshore, and so long as they do that without exceeding *de minimis* levels of US components or using technology controlled for national security purposes, they can continue to deal with Huawei. And that, of course, is true of relationships with any entity on the Entity List.’

‘The implications of being placed on the Entity List, although broader than the impact of an SDN listing in the sense that the Entity List applies to both US persons and foreign persons, are narrower in the sense that the prohibitions don’t apply to any and all dealings – only to exports, re-exports and transfer.’



Morgan Lewis



GLOBAL REACH

Global and domestic organizations face a daunting range of laws and regulations affecting how they conduct business. The ever-changing landscape of regulatory requirements presents companies with ongoing compliance challenges requiring timely, in-depth analyses.

Morgan Lewis's international trade and national security practice understands these requirements and advises clients on how to manage the full range of regulatory obligations in a cost-effective and practical manner. Across all industries—from defense to aerospace, to telecommunications, technology, and financial services—we partner with clients from start to finish, whether moving product, people, and technology in alignment with regulatory obligations or resolving government interactions with clients.

Giovanna M. Cinelli

Partner, Practice Leader | Washington, DC | giovanna.cinelli@morganlewis.com | +1.202.963.5619

Kenneth J. Nunnenkamp

Partner | Washington, DC | kenneth.nunnenkamp@morganlewis.com | +1.202.963.5618

www.morganlewis.com

© 2019 Morgan, Lewis & Bockius LLP | © 2019 Morgan Lewis Stamford LLC | © 2019 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

need for INSTEX. Matt Butter, an associate in the London office of Addleshaw Goddard, says that it 'could be a lifeline for getting some vital supplies into Iran – foods, medicines and humanitarian products etc. – where supplies are lawful under US

UK caretaker prime minister Theresa May for the poisoning of the Skripals in the English county town of Salisbury, Putin denied his country's responsibility, but added that traitors 'must be punished'.

Russia has not exercised the Trump

parapet in recent months. In March, Russian oligarch Oleg Deripaska sued OFAC claiming that it had 'unfairly targeted' him, causing losses of over \$7bn. And, in early July, a group of private equity outfits instructed law firm Latham & Watkins to bring an action against OFAC (*Intrater v OFAC*), their complaint arising out of what they describe as 'the warrantless seizure and ongoing interference with property interests of United States citizens by the Government through the operation of economic sanctions programs directed at foreign nationals.'

The harm to plaintiffs, it continues, has been 'magnified by the failure of the Government to issue authorizations to permit Plaintiffs to exercise their property rights...

'Specifically, OFAC has blocked and continues to deprive Plaintiffs of their ability to use, control and manage certain investment funds (the "Investment Funds") and the assets held by the Investment Funds, and to collect money that is due to Plaintiffs from the Investment Funds. OFAC has done so without any hearing or finding of wrongdoing by Plaintiffs, and without disputing that Plaintiffs are not themselves subject to sanctions.'

In essence, the plaintiffs jointly own investment funds which are also partly and indirectly owned by Viktor Vekselberg and the Renova Group – sanctioned by OFAC in April 2018 under an Obama-era executive order, and CAATSA.

The investment funds in question have been seized by OFAC under the 50% rule. But, say the plaintiffs, OFAC has issued no rules or guidance



'OFAC has always struggled with a backlog of licence applications. But that's exponential now. I've got licences pending since 2016 and that kind of delay is noticeable.'

Cari Stinebower, Winston & Strawn

sanctions. This would be of enormous benefit, vital, even, to the Iranian population and economy, given that the banks won't process payments for Iran – including where goods are firmly outside the scope of US sanctions. The US has made it clear that, outside of those "safe" categories of trade, it reserves the right to clamp down hard on INSTEX. Where non-US companies are looking to trade with Iran, the best thing they can do right now is to fully understand how secondary sanctions can be applied, to find workable payment routes, and to make sure they have contractual provisions in place so that if sanctions are removed or imposed, they can respond appropriately.'

That the good intentions of INSTEX are no guarantee of its effectiveness, Jane Shvets of Debevoise & Plimpton says: 'In any event, Iran sees INSTEX as insufficient to neutralise the effect of the US pull-out. And if Iran continues [to enrich uranium beyond limits agreed in the JCPOA] there's the possibility of a snapback of EU sanctions anyway.'

The Great [Bug]Bear

If Donald Trump and Vladimir Putin are figureheads of their respective nations, there were signs of US-Russian détente at the G20 meeting in Japan in late June. 'Don't meddle in our elections,' said Trump. Putin's eyes sparkled.

Sanctions – US and EU – have been in place against Russia for a number of years without eliciting any perceptible shift, either on the ground (Crimea remains firmly under the control of Moscow, not Kiev), or in attitude: at the same G20 meeting, admonished by

administration's energies in the way that Iran, China or Venezuela have – with Congress very much taking the lead in thinking up new Russia-related measures (like DASKA, PEESA and DETER). US energy secretary Perry has hinted at the prospect of sanctions that would impact upon the Nordstream2 pipeline – but this, points out Winston & Strawn partner Cari Stinebower, is a question of geopolitics:

'We're not going to see Putin pull out of Crimea anytime soon, it's just not going to happen. Nordstream2 has pitted Trump against Angela Merkel. Energy independence is a big issue. We've seen a lot in the press, but we'll have to see if anything gets through Congress.'

Pushing back

Historically, few entities or individuals have dared to challenge the might of the Office of Foreign Assets Control.



'Iran sees INSTEX as insufficient to neutralise the effect of the US pull-out.'

Jane Shvets, Debevoise & Plimpton

For one thing, it could prove costly to do so; for another, OFAC is always able to play the 'national security' card – against which it can be hard to push back without losing both credibility and credit.

However, two exceptions to the rule have raised their heads above the

explaining how US persons or entities can retrieve or access their property interests which are subject to sanctions, other than to apply for a licence – which the plaintiffs have failed to obtain despite their great efforts. To date, the suit says, 'OFAC have neither granted nor denied

Addleshaw Goddard LLP

Addleshaw Goddard LLP is a premium international business law firm, offering a full range of legal services, made up of over 1,100 lawyers operating from 12 locations around the world.

Our Corporate Crime and Regulatory Investigations practice includes dedicated specialist lawyers handling all aspects of international trade compliance matters. We have significant expertise advising FTSE 100 and FTSE 250 companies as well as other multinationals and SMEs in relation to EU and UK sanctions measures, export controls and supply chain compliance issues.

We act as the go-to contact point for a number of UK companies on operational trade compliance issues and support our clients in relation to regulatory investigations, enforcement actions and related litigation. In 2019 we were recognised by *Legal 500* as the UK's leading dispute resolution firm.

We have six offices in the UK as well as a presence in Hamburg, Dubai, Oman, Qatar, Hong Kong, and Singapore, plus a strategic alliance in Tokyo with Hashidate Law Office. We work seamlessly and in close collaboration with our preferred partner firms in other locations to deliver an international capability whenever and wherever required. We regularly work with some of the leading trade law practices in Washington D.C. in relation to US sanctions matters and are regularly called upon to advise US law firms and companies on matters involving EU and UK sanctions.

We are the UK representative of AT+ICA, the Association of Trade and Investment Controls and Compliance Attorneys, an independent network of leading trade compliance lawyers in Europe.

Our international trade capabilities include the following:

- advising on the latest EU and UK sanctions programmes and the impact of US sanctions on companies operating worldwide
- developing global trade compliance policies, third-party risk management and sanctions screening processes
- conducting international trade compliance audits and handling internal investigations
- preparing voluntary disclosures and liaising with regulatory authorities in relation to investigations and enforcement actions
- advising on all aspects of EU and UK military and dual-use export licensing requirements, including registering for, obtaining, and managing UK export licences

Milton Gate
60 Chiswell Street
London EC1Y 4AG

Phone: +44 20 7606 8855

Sanctions contacts:

Nichola Peters
nichola.peters@addleshawgoddard.com

Michelle de Kluyver
michelle.dekluyver@addleshawgoddard.com

Matt Butter
matt.butter@addleshawgoddard.com

www.addleshawgoddard.com



Crowell & Moring LLP

Crowell & Moring LLP is an international law firm with more than 550 lawyers representing clients in litigation and arbitration, regulatory, investigation, and transactional matters. The firm is recognised for its representation of companies in all aspects of international trade, as well as its ongoing commitment to pro bono service and diversity.

With lawyers in North America, London, and Brussels, and consultants in Asia, Crowell & Moring's International Trade Group advises clients on the full range of laws governing exports and reexports of goods, technology, software, and services. In conjunction with our full-service international policy and regulatory affairs affiliate, C&M International, and our international network of experienced, knowledgeable local counsel, we assist clients in gaining access to markets beyond the United States and the European Union (EU), including China, Hong Kong, Israel, and Singapore, as well as across Central and South America.

We provide legal insight and thought leadership highlighting significant trade developments via the Crowell & Moring International Trade Law Blog (cmtradelaw.com) and our This Month in International Trade newsletter (crowell.com/subscribe to sign up).

We know that our clients' needs, budgets, business models, and time frames vary, and our advice and compliance strategies are designed to meet each client's unique situation.

Our services include the following:

- Advising on licensing requirements and preparing licence and agreement applications
- Running internal investigations and assisting with voluntary disclosures
- Performing compliance audits
- Designing and implementing compliance programmes
- Performing jurisdictional assessments and preparing requests for commodity jurisdiction determinations
- Assisting in self-classification of products and preparing requests for commodity classification requests
- Performing export control/sanctions due diligence reviews related to proposed mergers and acquisitions
- Representing clients in civil and criminal enforcement proceedings
- Training on export control procedures and requirements

WASHINGTON, D.C.
1001 Pennsylvania Avenue NW
Washington, DC 20004-2595
Phone: +1 202.624.2500

Export controls contact:
 David C. (Dj) Wolff
djwolff@crowell.com
 +1.202.624.2548

BRUSSELS
7 Rue Joseph Stevens
Brussels, B - 1000
Belgium
Phone: + 32.2.282.4082

Export controls contact:
 Jeffrey L. Snyder
jsnyder@crowell.com
 +32.2.214.2834

LONDON
Tower 42, 25 Old Broad Street
London, EC2N 1HQ
United Kingdom
Phone: + 44.207.413.0011

Export controls contact:
 Michelle J. Linderman
mlinderman@crowell.com
 +44.20.7413.1353

www.crowell.com

crowell  **moring**

Plaintiffs’ applications. Plaintiffs remain in complete limbo, unable to control, manage, use, or dispose of their property.’

The case, says Cari Stinebower (herself a former OFAC lawyer), underscores a legalistic problem – i.e., the lack of clarity from the agency about how beneficial owners of trusts and foundations ought to be treated from a sanctions compliance standpoint, but also that OFAC appears to be overwhelmed by the workload that it’s created for itself.

‘OFAC has always struggled with a backlog of licence applications,’ she says, ‘But that’s exponential now. I’ve got licences pending since 2016 and that kind of delay is noticeable.’

Sometimes, she says, it’s possible for clients to receive informal interpretative guidance, or informal answers to questions. ‘But these are not binding and they leave transactions potentially exposed. What I’d like to see would be an increase in resources to OFAC so that, like Commerce, licence applications can be appropriately addressed and processed within six weeks.’

Indeed, complaints along these lines are commonplace. (Asked about rumours of low morale at the agency, one lawyer said, ‘OFAC has always been a very intense place to work, and badly paid. So, when the banks wanted new compliance people – as they do now – it was easy to raid.’)

Reach of the law

Overstretched as OFAC may be, it doesn’t tire of designating those that it deems deserve the full weight of US sanctions – part and parcel of efforts, coordinated with other agencies, both in the United States and abroad, to clamp down on perceived common threats.

Timothy O’Toole, member at DC law firm Miller & Chevalier, suggests that, if anything, the pace of multi-agency, multi-jurisdictional actions has picked up – in spite of the disalignment between the United States and many of its allies (e.g., the European Union and Canada) on trade and foreign policy issues.

‘It depends on the country, and it

depends on the issue,’ says O’Toole, ‘but we’ve seen a wave of enforcement actions that have drawn together OFAC, the Department of Justice, the Commerce Department, the New York Department of Financial Services – and sometimes non-US agencies, such as the UK Financial Conduct Authority and France’s enforcement bodies.’

O’Toole points to the November 2018 settlement with Société Générale (\$54m to settle apparent violations of the Iran Transactions and Sanctions Regulations, the Cuban Assets Control Regulations, and the Sudanese Sanctions Regulations) – part of a global settlement which also involved



‘We’ve seen a wave of enforcement actions that have drawn together OFAC, the Department of Justice, the Commerce Department, the New York Department of Financial Services – and sometimes non-US agencies.’

Timothy O’Toole, Miller & Chevalier

the board of governors of the Federal Reserve System, the US Department of Justice, the New York County District Attorney’s Office, the US Attorney for the Southern District of New York, and the New York State Department of Financial Services; and the more recent settlement with Standard Chartered, which saw OFAC levy a fine of \$600m for sanctions violations, and the UK Financial Conduct Authority simultaneously impose a fine of £100m for AML breaches.

‘Yes, to the extent that sanctions are enforced differently in Europe, there is little appetite amongst EU regulators for prosecuting US-led sanctions that they don’t support. But where it appears that there are no controls within, say, a financial institution, that’s different. For example, stripping information from Swift wires to remove the mention of sanctioned countries. Altering documents to fool enforcement agencies is something that no-one is going to look kindly on.’

Indeed, O’Toole says, such cases highlight the nexus between AML and

sanctions in practice: ‘In UK law, if you commit an act that represents a breach of AML regs, you’re obliged to report that to the FCA. If you have a US presence, that means there could also be a US law violation. That report might trigger US agents to follow up on it, and, often, where you have a problem in one area, it isn’t uncommon to find one in another area, especially where it stems from a lack of controls.’

Enforcement vac-eu-m?

Evidence of actual enforcement of EU sanctions regulations – including the blocking statute, aimed at preventing EU companies from complying with

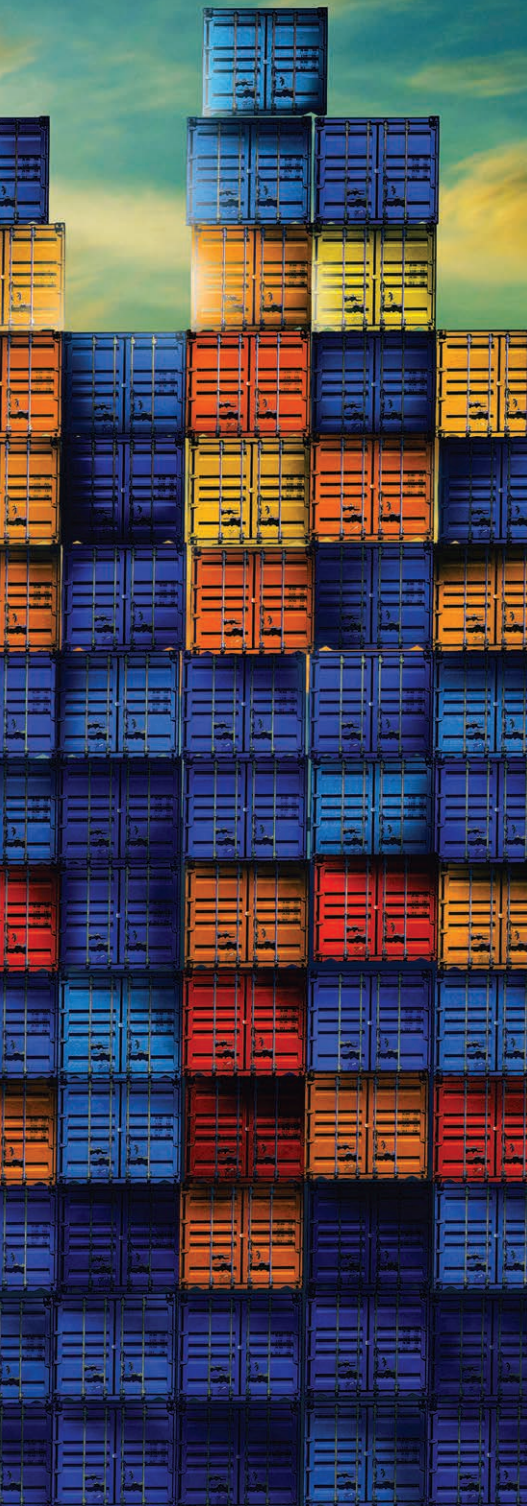
the sanctions laws of non-EU countries – remains elusive.

Mattias Hedwall characterises the state of play thus: ‘We’re not seeing a great deal of enforcement in the EU courts, but it is getting harder to get licences for activities that would otherwise be sanctioned from some of the regulators – like Germany’s BAFA and the ISP in Sweden. And while voluntary disclosure best practice does differ between Member States, it should be remembered that the authorities do speak to each other.’

Across Europe, says Jane Shvets, there is little indication that EU blocking regulation is being enforced. To date, she notes, the best known-case dates back to 2007, when charges were brought against an Austrian bank, BAWAG, which had closed 100 Cuban bank accounts to facilitate acquisition by a US private equity firm. And yet, she says, the most compliant companies still recognise the need to be ‘thoughtful and coordinated where multiple jurisdictions are involved.’

If or when the United Kingdom leaves the European Union, only time will tell the extent to which it finds itself in regard to its larger trading relationships. It is interesting that the first – and, to date, only – piece of legislation completed in readiness for Brexit is the Sanctions and Anti-Money





MARKET-LEADING INTERNATIONAL TRADE PRACTICE

Baker McKenzie specialises in the core areas of International Trade, such as export controls and sanctions, encryption issues, customs compliance, anti-bribery and anti-corruption, and also offers significant expertise in relation to WTO rules and free trade agreements. Our market-leading team is widely recognised by leading multinational companies and regulatory authorities as preeminent advisers for international trade work. We are increasingly appointed by clients with strong in-house teams to assist with high-profile trade compliance, customs, and anti-bribery matters.

UNSURPASSED GLOBAL COVERAGE

Our global coverage and structural integration is unmatched. We offer a 200-plus team of International Trade specialists who are strategically situated across more than 40 markets, including most of the world's key financial and policy centres such as Washington DC, London, Amsterdam, Frankfurt, Stockholm, Barcelona, Sao Paulo*, Mexico City, Hong Kong, Singapore, Beijing, and Sydney.

Multinational clients appoint us because of our unsurpassed ability to resolve multi-jurisdictional trade matters involving US, EU and other national regulatory regimes and authorities such as Germany, UK, China, and Australia.

INDUSTRY FOCUS

Our practitioners have a particular focus on industries that are most impacted by the introduction of new trade regulations, including major industrial manufacturers, energy, IT, telecommunications and financial services companies. We have a vast amount of experience advising many multinationals within the Fortune 100 and FTSE 100 communities.

GLOBAL THOUGHT LEADERSHIP

Our annual International Trade conferences in London, Amsterdam and Santa Clara are among the largest and best-attended trade seminars in the world. Clients also hail our regular globe trade webinars as an integral component of their trade compliance training.

Keep ahead of the curve on the latest economic and trade sanctions developments – visit the Baker McKenzie Sanctions Blog: www.bakermckenzie.com/sanctionsnews.

REGIONAL CONTACTS

EMEA

Paul Amberg, London
paul.amberg@bakermckenzie.com

Mattias Hedwall, Stockholm
mattias.hedwall@bakermckenzie.com

Sunny Mann, London
sunny.mann@bakermckenzie.com

Anahita Thoms, Dusseldorf
anahita.thoms@bakermckenzie.com

Asia Pacific

Jon Cowley, Hong Kong
jon.cowley@bakermckenzie.com

Kana Itabashi, Tokyo
kana.itabashi@bakermckenzie.com

Anne Petterd, Singapore
anne.petterd@bakermckenzie.com

Frank Pan, Shanghai
frank.pan@bakermckenzie.com

Americas

Nicholas Coward, Washington DC
nicholas.coward@bakermckenzie.com

Jose Hoyos-Robles, Mexico City
jose.hoyosrobles@bakermckenzie.com

Adriana Ibarra, Mexico City
adriana.ibarra-fernandez@bakermckenzie.com

Janet Kim, Washington DC
janet.k.kim@bakermckenzie.com

Alessandra Machado, Sao Paulo*
alessandra.machado@trenchrossi.com

John F. McKenzie, San Francisco
john.mckenzie@bakermckenzie.com

Bart McMillan, Chicago
bart.mcmillan@bakermckenzie.com

Manuel Padron, Juarez
manuel.padron@bakermckenzie.com

**In cooperation with Trench Rossi Watanabe*

www.bakermckenzie.com

Laundering Act 2018, which received royal assent on 23 May last year, ‘to enable the UK to comply with its international obligations and continue to use sanctions as a foreign policy and national security tool once the European Communities Act 1972 has been repealed.’

Even the UK’s Office of Financial Sanctions Implementation (‘OFSI’) – described by some at its inception as a ‘mini-OFAC’ – has yet to claim more than two scalps, neither of which could be described as major. It does, however, work hard to reassure its constituents that it’s on the case, or rather, pursuing many potential cases.

‘One area that everyone is looking at – but in particular the financial institutions – is Brexit. Will the UK have a “hard” Brexit? Will there be a transitional regime?’ says Jane Shvets.

There are, she says, differences between the new legislation and EU sanctions legislation which will become apparent further down the line.

‘The ownership and control test is broader under the UK Act. And, for example, under the relevant Russia restrictions, whereas previously EU subsidiaries of Russian companies were exempt from capital market restrictions, that exemption only applies to UK subsidiaries. That has a huge bearing on many funds from Cyprus, for instance.’

Matt Butter says that as regards OFSI, ‘There’s always potential for greater enforcement. It could bring a large number of actions. We’ve already seen the first waves of prosecutions coming through.’

In themselves, OFSI’s published actions are not likely to send tremors – or even a frisson – of fear through the financial services industry. There are two of them: one a fine (of a bank called Raphael & Sons) to the tune of £5,000; the other a fine (of £10,000) for global currency service provider Travelex. The reason for the fine in both cases was that they had dealt with funds belonging to a designated person – in breach of Council Regulation (EU) 270/2011 Egypt.

OFSI summarises its compliance and enforcement model thus: promote, enable, respond and change: ‘We promote and enable compliance through engagement and guidance. However where there is suspected non-compliance, OFSI responds by intervening to disrupt attempted breaches and by addressing breaches

From Russia – with a shrug...

WorldECR spoke with the Moscow-based general counsel of a Russian company, in a non-sensitive industry, which sells its products to around 70 countries. The company, he says, is scrupulous in its adherence to international sanctions, and while that does create challenges, it has not proved to be a hindrance to business – although it does make transactions more time-consuming.

‘Our company was always very sanctions-aware but, of course, everything changed in 2014 with the imposition of the Russian sanctions following the annexation of Ukraine. It does, potentially, affect every aspect of our business.’

‘One thing is that it demands the education of management and personnel, who invariably ask why a Russian company has to comply with US and EU sanctions. We also get similar responses from some of our Russian counterparties. And some people are not willing to do this. But my response is, “Since we are an international borrower, primarily, we have to accommodate the sanctions compliance clauses in lending clauses, because non-compliance would allow the banks to claim an early repayment of credit facilities, and if one bank were to do that, it would trigger early repayment rights to other lenders and that would be devastating.”

‘The funny thing is,’ he said, ‘that even Russian state banks are insisting on the inclusion of these sanctions clauses. Sometimes they’re actually tougher than the western banks. Back in 2014, if we couldn’t borrow from the western banks we could always borrow from Russian or Asian banks. It isn’t so straightforward nowadays.’

Vladimir Putin has of course threatened or promised to introduce regulation – in effect blocking laws – intended to steer Russian companies away from complying with non-Russian laws. To date they haven’t transpired.

‘The Russian government has discussed the imposition of regulations to “protect” Russian businesses, but in reality, that doesn’t make life easier. There’s a draft law in the state Duma, which would criminalise the disclosure of information to non-Russian authorities that would serve as a trigger for international

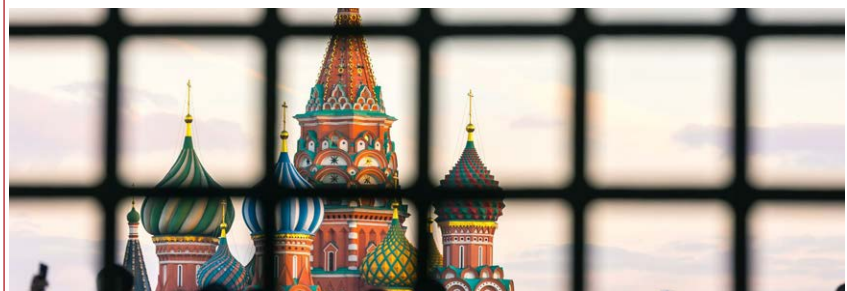
sanctions. I really hope it doesn’t go further. There’s another draft law which would prohibit compliance with international sanctions. So that would mean we couldn’t say to our counterparties: “We’ve terminated our contract because you haven’t been compliant with sanctions.”

‘Recently, it’s been proposed that there should be a law that would excuse sanctioned companies from giving some mandatory information, e.g., who its shareholders are, or its board members. But it would be very difficult for us to work with a company like that, because that is information we would need.’

‘As regards CAATSA [the Countering America’s Adversaries Through Sanctions Act], I wouldn’t say that it is stopping transactions, but it does complicate discussions with international companies. They now have much more sophisticated Know Your Customer procedures, and they’re asking for more information, and greater disclosure, often not directly connected with sanctions but relating to tax issues. Banks are closing accounts for companies in places like Cyprus, for example, that they would now treat as being “offshore”.

‘Now the most tangible risk that larger Russian companies face is the prospect of secondary sanctions being imposed. It means we have to be careful who we work with. Russian law doesn’t currently prohibit us from terminating negotiations with designated parties, though that might change.’

‘The reality is, the Russian market is getting used to this trading environment, and developing new instruments that allow business to continue – for example, introducing so-called alternative currency clauses: if the payment currency is in US dollars and new sanctions imposed that make that difficult, the contract is automatically transferred into new currency. And the demand for compliance advice is booming. Even for Russian companies that don’t have international parents. Many of them are employing new personnel, expanding their compliance departments and developing new procedures. I guess you could say, we’re adapting.’





Arent Fox

Practical Counsel. Unique Insight.

Transacting international business while complying with the myriad patchwork of US and international trade controls is an increasingly complicated endeavor.

Export Controls & Economic Sanctions Team



Kay C. Georgi
Partner, DC
202.857.6293
kay.georgi@arentfox.com



Marwa M. Hassoun
Partner, LA
213.443.7645
marwa.hassoun@arentfox.com



Regan K. Alberda
Counsel, DC
202.775.5771
regan.alberda@arentfox.com

**Smart In
Your World**

arentfox.com

effectively. We do this to change behaviour and to promote further compliance with financial sanctions.'

'Intervening to disrupt' is not of itself self-explanatory, but Matt Butter suggests that the way that the UK applies the Bribery Act, including its use of deferred prosecution agreements ('DPAs') (under which a prosecutor charges a company with a criminal offence but proceedings are automatically suspended if the DPA is

his firm is looking at 'new ways to do sanctions due diligence in a retail setting, putting in place compliance protocols as companies in these markets appreciate greater risk exposures, and banks become more cautious.'

Cross-border confusion?

Their experience underscores what arguably is the premise upon which *WorldECR* was first published: that

person [designated as an SDN under the order]."

'I know,' says Linney, 'that there are non-US companies who are not only unaware that this means that the sanctions potentially apply to them, but emphatically deny it!'

Which is why, she notes, the US State Department has been actively engaged in 'reaching out' to such companies to assure, if not reassure, them, of the extent of what could be described as its inclusiveness policy.



'In the context of Iran and North Korea, I think that secondary sanctions risk is very well understood. But less, for example, in the case of Venezuela.'

Barbara Linney, Baker Hostetler

approved by the judge), which would see more significant fines levied, is potentially an indicator of the direction of travel of the Office's strategy.

'I think that in time,' says Butter, 'it will tend to focus on high-value deferred prosecution agreements rather than criminal prosecutions. And if OFSI can encourage a culture of self-reporting, I think that's how it's going to work in the future.'

Matt Butter believes that in the UK awareness of the need for sanctions compliance is increasing, despite the apparent dearth of UK enforcement actions. 'Oil and gas, and of course defence companies, have always had to think long and hard about things like the sanctions risk presented by some markets. They're amongst our clients; but we're also working closely with FTSE 100 and 250 companies in sectors like manufacturing, pharma, retail, consumer and luxury goods. There's just a growing demand for specialist trade compliance advice.'

Butter's UK experience here is echoed by that of DC-based Hughes Hubbard partner Ryan Fayhee. One sector which, he says, is coming into the sanctions 'fold' (i.e., is increasingly looking for compliance advice) is 'luxury and high-end retail,' including jewellery, the art market and expensive cars. 'Changes in rules on ultimate beneficial ownership [pursuant to the Bank Secrecy Act] are really starting to fall into place now, and putting emphasis on Russian oligarchs.'

Their interest – and interests – in the luxury goods market, means that

compliance reflects the global nature of international trade and requires an awareness of the reach of the jurisdictions of multiple agencies, domestic, international, and transnational.

Companies' grasp of that requirement can be patchy, says Baker Hostetler partner Barbara Linney, who is frequently asked to advise on cross-border transactions for targets, acquirors and others.

'In the context of Iran and North Korea, I think that secondary sanctions risk is very well understood, but less so, for example, in the case of Venezuela. Many non-US companies view that sanctions regime as applying only to US companies. However, the relevant executive order does have a secondary sanctions element in the form of language that authorises blocking sanctions against persons doing business with the designated parties – i.e., "any person determined by the Secretary of the Treasury, in consultation with the Secretary of State...to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity or transaction [involving deceptive practices or corruption and the Government of Venezuela] or any

Shipping forecast

Perhaps paradoxically, a recent delisting case has shed some light on the vulnerability of non-US companies to that sanctions regime.

In early July, OFAC announced that it was delisting PB Tankers S.p.A., designated in April this year 'for operating in the oil sector of the Venezuelan economy'. Subsequently, said OFAC, PB took 'additional steps to increase scrutiny of its business operations to prevent future sanctionable activity.'

Ergo, PB Tankers was unblocked, freeing US companies to do business with it that they would not otherwise be able to do.

'The United States has made clear that the removal of sanctions is available for persons designated under E.O. 13692 or E.O. 13850...who take concrete and meaningful actions to restore the democratic order, including through refusing to operate in Venezuela's oil sector, which continues to provide a lifeline to the illegitimate regime of former President Nicolas Maduro,' the agency said, in announcing PB's reward for its good behaviour.



But, says Kay Georgi, the episode also raises important questions about who OFAC targets – and why:

'There's an issue around the use of secondary sanctions and its application,' says Georgi. 'Literally hundreds if not thousands of companies may have provided what could be interpreted as "material support" or engaged in "significant transactions". So the natural question becomes who should OFAC choose when it has near limitless scope? Clearly, some targets

Glimpsing 18 months of OFAC activity

WorldECR asked Dr Pascal Ditté of sanctions-intelligence.com for statistics relating to sanctions activity in the past 18 months and if he might consider

- How have US sanctions evolved over the past 18 months?
- How often did the OFAC SDN List change and which areas were most affected?
- What are the implications for sanctions screening?

According to Dr Ditté's research:

- Between January 2018 and June 2019, the size of the OFAC SDN List grew by 29.3% to a total of 7,725 entries.
- The frequency of list changes is high: The SDN list changed 124 times during that period, the equivalent of one list change every 4.4 calendar days on average.
- Each list change includes a number of amendments to the entries on the list: In total, there were 2,753 amendments identified, which are divided into 1,796 added entries (65.2%), 911 changes of existing entries (33.1%) and 46 removed entries (1.7%).

- The increase in the size of the OFAC SDN List of 29.3% was to a large extent due to the re-imposed sanctions on Iran: Iran-related sanctions made up 51.8% of all new 1,796 entries. The share of the remaining 48.2% is split between Global Terrorism Sanctions Regulations (16.4%; here the majority of the new entries are also Iran-related), Venezuela-related (7.8%), Narcotics Trafficking Sanctions (6.6%), DPRK-related (6.8%), Ukraine-related (5%), and others (5.2%).

Screening challenges

Due to the high frequency of list changes, there is a risk of unintended sanctions breach, particularly in high-volume transaction screening, if lists are not kept up to date in the screening systems. The figure above of 4.4 days between OFAC SDN List versions is an average value only. Sometimes lists change every day – or even twice a day.

Indeed, the sheer volume is a major factor. 1,794 additional entries or a 29.3% increase in 18 months is a big number in itself – but when it comes to the number of names to screen, this figure needs to be multiplied as most entries have additional

alias names or address information that need to be taken into account as well.

In addition, each party that is scanned in the screening processes needs to be checked if it falls under the OFAC 50% rule and is owned or controlled by one of the (newly added) SDN-listed parties. All this means additional workload in the screening process and a number of additional true hits and false positives that have to be sorted out (often manually).

Do also bear in mind that the analysis above refers only to the US OFAC SDN List. There are, as readers will know, other relevant US sanctions lists as well. Thus, the volume of US lists is even higher.

The fall-out

What are the consequences for companies? The figure of a nearly 30% list size increase in the last 18 months would suggest that organisations ramp up their staff and technical resources accordingly in order to avoid bottlenecks or worse.

This is a summary of the current OFAC SDN 18-months analysis. The full analysis is available to subscribers of www.sanctions-intelligence.com.

are too big, but is it right that to choose smaller ones for whom an SDN designation could literally be a death knell? And how can OFAC go after one entity without appearing discriminatory, given that there are so many companies that might also meet the threshold?

Mayday!

‘There are huge questions raised when vessels [like those owned by PB Tankers] are designated. The P&I

who routinely advises ship-owners, insurers, charterers and others on sanctions in a maritime context.

‘Everyone perceives entities [on OFAC’s SDN list] to be the “bad guys”. But where ships are designated, the knock-on effect in the insurance market is huge and innocent third parties can be caught in the cross-fire with no-one to pursue for their claims or for unpaid costs.’

Interestingly, adds Linderman’s colleague Jeff Snyder, the strategic use

once they have. It’s something that they’ve become very skilled at doing.’

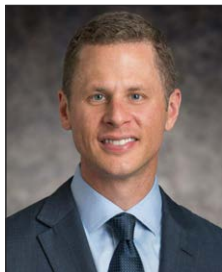
2020 vision

Looking to the future, sanctions lawyers suspect that their practices can only flourish if the uncertainties and conflicting policy agendas amongst former allies continue. (‘Unless, of course, sanctions become so complex, mutually-negating and haphazardly enforced that companies stop bothering to comply,’ adds one.)

But, murky as the future always is, here are some steers from the lawyers who have been generous enough to share their thoughts with *WorldECR* for the purposes of this report.

Pyongyang ping-pong

Donald Trump and Kim Jong-un may continue to send each other beautiful letters and make landmark gestures but there’s no indication of anything remotely like an agreement emerging from the frenemyship (and North Korea’s reputation for human rights violations continues to be as appalling as it ever was). From a compliance perspective, North Korea sanctions were once regarded as obscure, in effect orphaned by the implausibility of




‘Lots of companies are now rethinking their supply chains and being extra cautious with Chinese vendors.’

Ryan Fayhee, Hughes Hubbard & Reed

clubs, the insurers have to ask themselves: “Can we insure them? Can we pay claims?” It’s a particular headache for people dealing with claims dating back to before the SDN listing,’ says London-based Crowell & Moring partner Michelle Linderman,

of explicitly on-off sanctions to encourage good behaviour mirrors one from another OFAC ‘playbook’: enforcement of the Kingpin Act, ‘where you see people designated, “encouraged” to provide useful information, and the designation lifted

Hughes Hubbard & Reed

A flashlight is shown in the top right corner, pointing towards a globe of the world. The flashlight's beam illuminates the globe, which is rendered in a light, textured style. The background is a light gray gradient.

World-Wide Experience Trusted Compliance Advice Global Sector Strength

We represent many of the world's leading international businesses, providing advice on compliance with applicable extraterritorial sanctions, export and re-export controls, and anti-money laundering rules. We are experienced and trusted advocates in conducting internal investigations and shepherding our clients through complex compliance audits, voluntary disclosures, and civil and criminal enforcement actions before the Commerce, State and Treasury Departments and the Department of Justice. We also represent foreign and U.S.-based businesses in transactions subject to review by the Committee on Foreign Investment in the United States (CFIUS), as well as in transactions involving classified information requiring Foreign Ownership, Control, or Influence (FOCI) review.

Our team includes experienced attorneys, many of whom have held prior positions at key government agencies, who are thought leaders within their fields. Through our core teams based in Washington, D.C. and Paris, we offer practical, business-oriented advice from a global perspective.

**“Hughes Hubbard has
an especially strong U.S.
investigations practice.”**

—Global Investigations Review, 2018

**“There’s a strong reliance
upon a collaborative
approach.”**

—Chambers USA

We serve our global clients through our offices in the U.S. and Paris, and through our cooperation agreement with Saud Advogados in Brazil and our longstanding relationships with leading local firms in countries across the world.

Ryan Fayhee • Washington, D. C.
+1 (202) 721-4691
ryan.fayhee@hugheshubbard.com

Roy Liu • Washington, D. C.
+1 (202) 721-4621
roy.liu@hugheshubbard.com

Olivier Dorgans • Paris
+33 (0) 1 44 05 79 68
olivier.dorgans@hugheshubbard.com

Lynn G. Kamarck • Washington, D. C.
+1 (202) 721-4760
lynn.kamarck@hugheshubbard.com

Alan G. Kashdan • Washington, D. C.
+1 (202) 721-4630
alan.kashdan@hugheshubbard.com

doing business with the country, sanctions regardless.

Recent developments put a different cast on it.

‘When I was working for government,’ says Ryan Fayhee, a partner at Hughes Hubbard & Reed and who spent ten years of his career at the Department of Justice, ‘I’d thought we’d isolated North Korea to the extent that it was possible to do. I’d probably underestimated the country’s ability to export labour – and for Chinese banks to facilitate North Korean business. One of the issues we’ve followed closely is the intensive focus on Chinese banks operating in US dollars. It certainly has a bearing for companies receiving payments from Chinese banks. Lots of companies are now rethinking their supply chains and being extra cautious with Chinese vendors.’

The case of E.l.f. Cosmetics looms large in this respect. In January, the Californian company paid just short of \$1m to settle potential liability for 156 apparent breaches of the North Korea Sanctions Regulations – each, a shipment of false eyelash kits from Chinese suppliers which contained materials from the DPRK.

‘Chinese products are very prevalent in the supply chain. E.l.f. didn’t know it was doing anything wrong, it just didn’t look at its supply chain,’ says Tim O’Toole. The procedures that were lacking were a thorough risk assessment, and repeated audits for sanctions violations.’

Amongst the measures that the company took to ‘minimize the risk of

‘The first of those “steps” might raise the eyebrows of an EU lawyer, it must be said,’ suggests one EU lawyer.

Reporting for duty

On 20 June, OFAC published a (seemingly innocuous) amendment to its Reporting Procedures and Penalties



‘Policy changes on a whim but the consequences of breaching the law have not.’

Alison Stafford Powell,
Baker McKenzie

Regulations, which, it said, ‘Provided updated instructions and incorporates new requirements for parties filing reports on blocked property, unblocked property, or rejected transactions; revises the licensing procedures section to include information regarding OFAC’s electronic license application procedures, and to provide additional instructions regarding applications for the release of blocked funds; and clarifies the rules governing the availability of information under federal law, including the Freedom of Information Act (FOIA), for information that is submitted to OFAC in connection with blocking or unblocking reports, reports on rejected transactions, or license applications.’

On the face of it, a minor change to reporting requirements, but one, which

investigation or enforcement. Because OFAC is heavily reliant on voluntary or required reports, as well as referrals from agencies or media reports for its leads.

‘The rule change on the reporting standard means that all US persons are now required to file a reject report.

Previously, it only applied to financial institutions – not companies. This means that if I’m a US company, as distinct from, say, a bank, and I get a request from a potential customer and I realise that that person or entity is an SDN, I have to report it. Not only are the practical implications of this standard potentially material to many company’s compliance programmes, but now a lot more people are going to be in front of OFAC, and that can often lead to more follow-ups.’

This, potentially, is a headache compounded by the fact that, as Baker McKenzie partner Alison Stafford Powell points out, ‘The trend of the US sanctions has been toward the unpredictable – increasingly becoming the norm. Policy changes on a whim but the consequences of breaching the law have not. Enforcement is stricter, as are the expectations of compliance, yet there is often little or no grace period to react or to withdraw or cancel contracts or deals before new restrictions are implemented. Questions about policy are not answered.’

Increasingly, she says, the sanctions-compliant community is asking what underpins policy: ‘I have clients who have had repeat licences for non-sensitive business withdrawn. Is this because there’s a shift toward sanctions as a “national security” tool in support of promoting economic objectives and technological advantage rather than foreign policy?’

Needed guidance

But for all the OFAC-bashing that lawyers are inclined toward, the publication in late June of guidance by the agency on its expectations of



‘[The OFAC guidance] really is to be welcomed, because it consolidates 30 years’ worth of practice by OFAC, and says, “This is what we care about.”’

Giovanna Cinelli, Morgan Lewis

recurrence of similar conduct,’ were the adoption of new procedures ‘to require suppliers to sign certificates of compliance stating that they will comply with all U.S. export controls and trade sanctions,’ and to ‘conduct an enhanced supplier audit that included verification of payment information related to production materials and the review of supplier bank statements.’

Crowell & Moring partner Dj Wolff points out, strikes at the heart of an important question: Of all the many leads that OFAC receives, which does it follow up?

‘OFAC’s policy posture is that they’re supposed to be going after the bad actors and the biggest cases,’ says Wolff. ‘The reality is that, when people put themselves in front of the agency, they put themselves at risk of

companies' compliance efforts has met with approval. The 12-page document outlines what OFAC requires in terms of senior management commitment (including, for example, the desirability of appointing a dedicated OFAC sanctions compliance officer). It includes advice on promoting a 'culture

And yet – as the world takes stock of the first two quarters of 2019 and looks forward to the shiny future – it's clear that such guidance may provide preventative medicine for many compliance ills. Though not all of them. The United States, its president and agencies may possess a lead position in

throughout their supply chain, without being added to it.'

Under the proposed law, companies that avoid business with Chinese companies in compliance with, for example, US law would be placed on this list, though the Chinese government has yet to specify what consequences might lay in store for them.

And, points out Snyder, there may be actions taken by governments that take a leaf out of the US book without necessarily being intended as pointed, tit-for-tat measures, which nonetheless create new compliance traps (viz. export controls imposed by Japan on South Korea, related to South Korea's recent rulings on compensation it believes ought to be paid by Japanese companies for forced labour between 1910 and 1945).

'It isn't our job,' said one lawyer, 'to tell our clients what is going to happen in the future. Setting yourself up as some kind of seer or oracle is to set yourself up for a fall. But we can help them think through some of the possibilities and repercussions – so that when things come up, as they will, they can respond quickly with minimum disruption.'

This, said the lawyer, is as much as anyone can do. ■



'Other countries are looking at the success of agencies like OFAC and the Bureau of Industry and Security and thinking about how they can be emulated.'

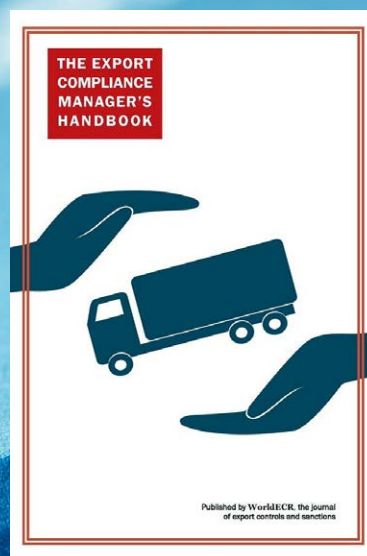
Jeff Snyder, Crowell & Moring

of compliance', on conducting risk assessments (especially during M&A activities), on auditing, training, and implementing internal controls.

'This really is to be welcomed,' notes Giovanna Cinelli, 'because it consolidates 30 years' worth of practice by OFAC, and says, "This is what we care about." It represents a higher degree of seriousness from the Treasury, and underscores the extent to which the president favours foreign policy-type solutions to the country's challenges.'

the global pecking order, but others cannot be discounted. As Crowell & Moring's Jeff Snyder observes: 'Other countries are looking at the success of agencies like OFAC and the Bureau of Industry and Security and thinking about how they can be emulated. We're seeing the prospect of countervailing measures being taken by Russia, and in May, China's Ministry of Commerce announced that it would be introducing its Unreliable Entity List. Companies will be asking themselves how they can ensure compliance

Books from the publisher of WorldECR



Available now from www.worldecr.com/books

Recent OFAC policy changes and settlement trends suggest shifting enforcement priorities

By Ryan Fayhee, Roy (Ruoweng) Liu and Alan Kashdan

In 2019, the US Department of the Treasury, Office of Foreign Assets Control ('OFAC') has indicated, through public announcements and settlement agreements, that it has shifted its focus concerning some aspects of the agency's enforcement actions. Two recently announced policy changes suggest that OFAC will increasingly emphasise the importance of a company's programmatic sanctions compliance when determining its response to a company's violation of sanctions rules. In addition, recent enforcement trends suggest that OFAC is examining a more diverse set of enforcement targets, including companies in industries that have not previously been scrutinised, and the foreign subsidiaries of US parent companies.

Sanctions compliance in assessing penalties for sanctions violations

At a June 2019 meeting of the American Bar Association, OFAC Director Andrea Gacki stated that the agency would no longer credit all types of fines paid in multi-agency joint settlements, but only fines for 'the same pattern of conduct for the same period of time' that would give rise to sanctions violations. Although Ms. Gacki said the change was designed to balance 'unnecessary piling-on' with 'a strategic use of its enforcement authorities,' the effect of the revised policy is likely to lead to higher cumulative penalties. Indeed, Ms. Gacki noted that this new policy was reflected in two settlements in April 2019 that each resulted in penalties in excess of \$600m. By limiting the credit it will give for settlements with other agencies only to conduct that would have given rise to an OFAC sanctions violation, the policy ensures that attention to sanctions compliance will not be an afterthought and that all conduct, not simply egregious conduct satisfying the 'willful' intent threshold, will be captured and accounted for. Many of OFAC's sister agencies typically involved in multi-agency settlements are focused on related cross-border compliance issues, such as anti-bribery and corruption, anti-money laundering, and export controls. Moreover, DOJ may only prosecute sanctions conduct that is knowing and willful, whereas OFAC may issue civil fines and penalties on a strict liability basis. OFAC has made clear that all sanctions violations will be pursued

with force equal to related compliance areas, and should accordingly be given the same attention by companies in their compliance efforts.

Second, focusing on a company's compliance efforts, in December 2018 Under Secretary of the Treasury for Terrorism and Financial Intelligence Sigal P. Mandelker announced that OFAC would be issuing guidance on sanctions compliance programmes and that, '[g]oing forward, these types of compliance commitments will become an essential element in settlement agreements between OFAC and apparent violators'. On 2 May 2019, OFAC published these guidelines, entitled A Framework for OFAC Compliance Commitments ('Compliance Commitments'), which provide companies a framework for how to establish a comprehensive sanctions compliance programme. The guidance identifies 'five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training'. Additionally, the publication – along with recent enforcement actions – indicates that such programmes could be mitigating factors in settlement agreements if violations do occur.

One purpose of the Compliance Commitments could be to encourage all companies to re-evaluate the sufficiency of their existing programmes. In a section identifying root causes of OFAC sanctions violations, the Compliance Commitments explain: 'OFAC has finalized numerous civil monetary penalties since publicizing the Guidelines in which the subject person's lack of a [sanctions compliance program] was one of the root causes of the sanctions violations identified during the course of the investigation. In addition, OFAC frequently identified this element as an aggravating factor in its analysis of the General Factors associated with such

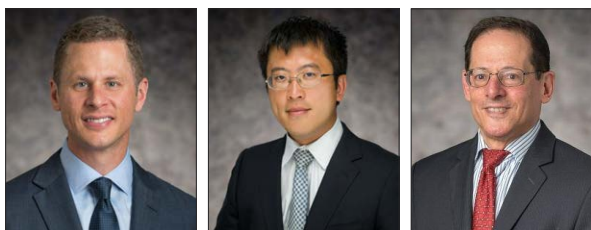
administrative actions.'

Broadening the focus of enforcement

Recent OFAC enforcement trends suggest that the agency is increasingly broadening its enforcement focus to new areas. Whereas OFAC's enforcement efforts in the past few years may have prioritised financial institutions, now that banks may have 'gotten the message', more recent enforcement actions have targeted a more diverse group of companies, including companies operating in the cosmetics, tourism, transportation, engineering, chemical, and software and technology industries in 2019 alone. This widening enforcement net underscores that all companies, regardless of size or industry, should make a serious effort to comply with US sanctions rules and regulations.

Further, although holding companies liable under the doctrine of successor liability is not a new concept, enforcement actions stemming from successor liability are a growing area of focus for OFAC. Of 14 enforcement actions so far in 2019, three have involved non-US companies acquired by US companies that continued to engage in prohibited transactions with sanctioned entities post-acquisition.

OFAC's recent policy changes and enforcement trends indicate that the agency is widening its enforcement focus. Based on these changes, we expect civil monetary penalties for sanctions-related conduct in multi-agency settlements to grow. We also expect non-traditional companies involved in international business to be increasingly subject to the same scrutiny as traditional financial enforcement targets. Companies that have even a small amount of exposure to US sanctions liability should ensure that they have adequate compliance procedures in place that follow the Compliance Commitments referred to above. ■



Ryan Fayhee and Roy Liu are partners at Hughes Hubbard & Reed where Alan Kashdan is counsel.
hugheshubbard.com

Reforming US secondary sanctions: What's wrong that can be righted?

By Kay C. Georgi, Marwa M. Hassoun and Regan K. Alberda

In a nutshell, US secondary sanctions are the sanctions that the United States can apply to wholly non-US actors in wholly non-US transactions of which the US administration disapproves. Numerous statutory and executive orders provide authority for imposing secondary sanctions for transactions involving multiple countries, primarily Iran, Russia, North Korea and Venezuela, and involving a wide range of activities, including violating human rights. Many of these authorities include the 'nuclear option' of placing the sanctioned individual or entity on the SDN list. None of these authorities include a well-defined numerical threshold for imposing sanctions, with many requiring sanctions for 'significant transactions' or providing 'material support'. The US administration has identified many persons and entities for sanctions or placed them on the SDN list under these authorities.

So what's wrong with this? We do not want to debate the goals of economic sanctions or whether they are preferable to the use of military force, but only to identify some problems with the application of secondary sanctions:

1. The triggers for secondary sanctions are unclear: What is a 'significant transaction'? OFAC's FAQ 542 tells us:

'OFAC will consider the following list of seven broad factors that can assist in the determination of whether a transaction is "significant": (1) the size, number, and frequency of the transaction(s); (2) the nature of the transaction(s); (3) the level of awareness of management and whether the transaction(s) are part of a pattern of conduct; (4) the nexus between the transaction(s) and a blocked person; (5) the impact of the transaction(s) on statutory objectives; (6) whether the transaction(s) involve deceptive practices; and (7) such other factors that the Secretary of the Treasury deems relevant on a case-by-case basis.'

2. There's no one to ask. Non-US persons

who are not subject to US jurisdiction cannot apply to OFAC for a licence. And while OFAC tries to answer questions posed to its compliance hotline, it is a small department and there are understandably a lot of people asking questions. Additionally, the guidance from one OFAC representative is not generally binding upon OFAC itself.

3. Secondary sanctions are actually imposed in a discriminatory fashion. This is not intended as a criticism: it takes time and money to build up a file supporting the imposition of secondary sanctions. Even a fully-unded sanctioning authority cannot possibly keep up and decisions on whom to target must be made.

4. Placing a person or an entity on the SDN list is a nuclear option. It is not merely a question of doing business with Iran or doing business with the United States. Indeed, an entity on the SDN List will have problems doing business in its own country, due to risk-averse positions taken by banks and other companies, which have only been exacerbated by the risk of secondary sanctions. We know of one company that was almost bankrupt by the time it was removed from the SDN list, and that company had minimal US business.

5. There often is no warning. In many cases, the US government has reportedly reached out to the non-US company or government and said, 'Hey, what you are doing is lining you up for secondary sanctions, cut it out.' It has certainly been warning the Turkish and Indian governments not to purchase the Russian S400 missile system. But SDN blocking sanctions are effective only if imposed with no warning at all. So the individuals and companies that are placed on the SDN list often wake up in the morning to find their assets have been blocked.

6. Getting off the SDN list is very difficult and takes time and resources. In some cases, parties cannot be removed from the list for a particular period of time. Often parties end up hiring US counsel in order

to facilitate their removal from the SDN list.

7. Secondary sanctions do not usually trigger standard *force majeure* clauses. Non-US companies cannot tell customers that they cannot perform binding contracts because the United States has imposed secondary sanctions: they are not legally compelled to comply with US secondary sanctions laws.

8. Secondary sanctions commercially favour the non-compliant. When companies that do not wish to trigger secondary sanctions find some means to step aside, the companies who step in are those that do not care about US foreign policy or the US market.

So does this have to be the case? We think not – some possible solutions might be:

- 1.** Adopt clear and high thresholds for investments and transactions, and clear descriptions of conduct.
- 2.** Provide clearer guidance to non-US parties. If the Department of Commerce can develop a decision tree for 'specially designed' why can't something similar be done in the sanctions area?
- 3.** Require secondary sanctions be applied to investments and transactions above a certain amount, no matter the actor.
- 4.** Do not require the secondary sanctions to be SDN sanctions. There are many sanctions options that bite but do not put a company or individual out of business.
- 5.** Provide fair warning to the target and allow it to change its course. If the purpose of the sanctions is to change conduct, this is key.
- 6.** Provide a clear path for the removal of secondary sanctions. If you agree to X, you are removed from the SDN List.
- 7.** Provide a written warning of impending sanctions that the target can use to try to get out of the problematic contract, if applicable. Having a written statement from a government authority can help companies to exit contracts.

Doing so will ensure that less compliant companies do not benefit from the discriminatory application of secondary sanctions by engaging in the very conduct the United States wishes to discourage. ■

We would like to thank Baerbel Sachs of Noerr LLP whose speech at the European Association of Trade + Investment Controls and Compliance Attorneys conference in Milano, Italy on 21 June 2019, inspired this article.



Kay C. Georgi and Marwa M. Hassoun are partners at Arent Fox where Regan K. Alberda is a counsel.

www.arentfox.com

Navigating the swamp: staying competitive during a resurgence of export controls

By Jeff Snyder, Michelle Linderman and Dj Wolff

There's an old saying that to get through the swamp, you do not have to kill all the alligators. The adage is a useful reminder to today's compliance officers as they seek to navigate the ever-changing (and seemingly expanding) sanctions and export control compliance environment. That means knowing on what to focus, what the rules really mean, and how to execute a risk-based efficient compliance programme.

The challenge is that in today's landscape, it is no longer enough to simply know the rules and manage around that risk. In a world with multilateral, aligned controls, compliance is intellectually straightforward, if sometimes practically challenging. The hardest decisions are often whether to adopt a lower-risk 'least-common denominator' approach, reducing risk but sacrificing business, or seek to maintain a more sophisticated programme tailored to jurisdictional differences.

Today, this alignment is fraying as countries increasingly take steps to counter what they perceive as extra-territorial US measures. The EU has expanded its 'blocking' statute to prohibit compliance with all US 'secondary' sanctions on Iran – with at least one Member State purportedly initiating enforcement in late 2018 – and created a government-sponsored financing mechanism, INSTEX, to bypass the US financial system. Russia has built on the 'counter-sanctions' it has maintained since 2014 and is debating legislation modeled on the EU blocking statute. And China, in response to US Entity List designations of Chinese telecommunications and super-computing companies, has dusted off and proposed a new 'unreliable' list of its own.

These conflicts arise throughout the operations of a global company, but the three areas below present key risks:

- **Global navigation of rules**

Most obviously, global business now requires global compliance. Global compliance may be driven by US or EU sanctions, but often requires a matrix of other national laws – managing competing obligations can mean complex questions of contract law, and disputes. And this analysis is no longer as straightforward as it once seemed. For example, while OFAC has historically asserted jurisdiction on the

basis of US dollar 'clearing', the UK's Office of Financial Sanctions Implementation ('OFSI') has quietly issued guidance that it has the same jurisdiction over anything that clears through a UK-based financial institution.

- **Mergers & Acquisitions ('M&A')**

M&A has always presented significant trade risk as different businesses, subject to different jurisdictional requirements and compliance cultures, seek to create an enterprise-wide programme. Recently, however, the regulatory attention has only increased. It is no longer enough to include trade in the M&A due diligence toolkit. Historic breaches can adversely impact the value of a business and early identification of risk issues enable an acquirer to correctly value the target, mitigate future risk, or walk away if the downside outweighs the benefit of the acquisition. But, if the deal proceeds, regulators now expect that the new parent company will follow-through on the conditions imposed at closing, building out compliance programmes and, critically, auditing compliance by the new affiliate.

- **Global investigations**

The spectre of a global investigation – whether internal or government-facing – with its document reviews, interviews, and potentially seven-, eight-, or nine-figure penalties has long weighed on global compliance officers. That risk has only increased recently, as the compliance attention has moved off of financial institutions to the broader community. From the largest export control penalty in history to multi-jurisdictional anti-bribery and anti-corruption ('ABC') investigations, the US enforcement lens is widening. Worse, other regulators are following suit, as EU Member State anti-money

laundering ('AML') authorities have issued several billion-dollar penalties, while OFSI has announced it is currently reviewing at least 122 reported breaches of financial sanctions. Managing a global investigation is no longer a skill required only of a financial institution's sanctions officer.

So what can be done? We have a few suggestions:

- **Stay alert to change**

Given the increasing number of new restrictions, compliance programmes must be agile and able to integrate and adapt to potentially changing rules to be able to maximise business opportunities while avoiding future costly investigations or enforcement actions.

- **Integrate compliance functions**

Given how governments are increasingly viewing export controls and sanctions, let alone AML and ABC, as tools in the same foreign policy toolkit, compliance officers must be equipped to understand, and react, to the entire landscape. While that does not necessarily require one person with expertise in each field, it does require breaking down silos that many companies have created within compliance, to ensure seamless communication across functions.

- **Hire advisors with industry expertise**

In a world in which it is no longer sufficient to simply know the rules, it is no longer sufficient to rely on advisors who repeat those rules. Guidance in the current regulatory environment requires a deep industry knowledge to understand how to integrate ever more complicated requirements into the realities of a business, whether that be insurance, shipping, manufacturing, or finance. ■



Jeff Snyder, Michelle Linderman and Dj Wolff are partners at the law firm, Crowell & Moring.

www.crowell.com

Trading tariffs for sanctions?

By Barbara D. Linney

While following presidential tweets may have replaced reading tea leaves as a method of predicting the future of US trade policy, President Trump's latest remarks on trade negotiations with China drew quick reminders from both the administration and Congress that a Twitter account does not have the force of law. His suggestion, following a recent meeting with the president of China, that Huawei would be removed from the Entity List prompted a directive from export enforcement officials that the export ban and policy of denial remain in place and was met with vows by powerful senators on both sides of the aisle to reverse de-listing with legislation.

One such senator, Marco Rubio, who has been an outspoken critic of using Huawei as a 'bargaining chip' in China trade negotiations, also has co-sponsored legislation that would restrict certain trade with China and authorise sanctions against persons who engage in unauthorised transactions. The China Technology Transfer Control Act of 2019 (S. 1459) was introduced on 14 May 2019 and referred to the Senate Banking Committee. While not targeting Huawei specifically, it defines 'technology' broadly to include 'goods or services relating to information systems, Internet-based services, production enhancing logistics, robotics, artificial intelligence, biotechnology, or computing.'

The pending legislation makes clear that while President Trump may have taken additional tariffs on Chinese imports off the table – at least for now – Congress remains focused on potential threats to US national security and determined to deploy both export controls and sanctions in response.

If passed, the legislation would require the US Trade Representative to publish a list of products manufactured or produced in, or exported from, China that receive support from the government under the Made in China 2025 policy or otherwise receive government support and 'have or will in the future displace net exports of like products by the United States.' The list must also include products determined by the Secretary of State to be used by the Chinese government to carry out human rights or religious freedom violations.

Although the draft legislation includes somewhat clear direction on products to be identified as supported under the China 2025 strategy, no guidance is provided regarding what other forms of

government support might lead to inclusion on the list, although items in this category must meet the additional requirement of displacing US exports.

Finally, the list must include products from 16 enumerated industries, including several industries subject to the Critical Technology Pilot Program implemented in

Congress always seems willing to pull export controls and sanctions out of its toolbox whenever it perceives that trade or foreign policy threatens national security.

2018 by the Committee on Foreign Investment in the United States.

'Technology' or 'intellectual property' that is a component of production of the newly listed products – along with certain other technology or intellectual property – would be required to be controlled under either the International Traffic in Arms Regulations ('ITAR') or the Export Administration Regulations ('EAR'). 'Intellectual property' is broadly defined to include property protected by copyright or patent or registered as a trademark, as well as trade secrets and 'any other form' of intellectual property. Although far from clear, it appears that this definition may be intended to override the ITAR and EAR carve-outs for 'publicly available' technology.

Also falling within the definition of controlled 'covered national interest technology or intellectual property' would be technology or intellectual property that

- would make a significant contribution to China's military potential that would prove detrimental to US national security;
- is necessary to protect the economy of

the United States from the 'excessive drain of scarce materials and to reduce the serious inflationary impact of demand' from China; or

- is used by the Chinese government to carry out human rights violations or violate religious freedoms.

Exports or re-exports to, or transfers in, China of covered national interest technology or intellectual property would be subject to ITAR or EAR controls. As the legislation is silent on licensing policy, it appears that the drafters intend that the export agencies would set licensing policy in the implementing regulations – subject, of course, to mandatory application of the arms embargo against China.

In addition to facing enforcement actions for violations of the new controls, foreign and Chinese persons would be subject to mandatory sanctions under IEEPA in the form of asset-blocking – i.e., addition to the SDN List. No finding of 'national emergency' would be required. Sanctions would be imposed against (a) foreign persons who knowingly sell or otherwise provide to, or purchase from, China, any covered national interest technology or intellectual property subject to US jurisdiction, and (b) any Chinese individual or entity who knowingly uses such technology or property obtained in violation of the new export controls. The first category of sanctions appears to be required irrespective of whether export authorisation has been obtained, but this may be a drafting oversight given the direction to 'control' exports as opposed to banning them outright.

While this legislation is not and may not become law, it does serve as a reminder that Congress always seems willing to pull export controls and sanctions out of its toolbox whenever it perceives that trade or foreign policy threatens national security. Whether the long-term impact of this strategy will be helpful or harmful to national security remains to be seen – and as hotly debated as ever. ■



Barbara D. Linney is co-leader of the International Trade team at Baker Hostetler in Washington, DC.

www.bakerlaw.com



THE GOING GETS TOUGH

Compliance professionals share their experiences of how different industry sectors are coping with recent sanctions and enforcement developments and offer suggestions on how the challenges can be mitigated.

Businesses with a global footprint have had to process a proliferation of major sanctions and enforcement developments in the past 18 months, mostly driven by US foreign policy goals. *WorldECR* asked a number of experienced compliance professionals in a range of global industries – including oil and gas,

technology, and logistics – for their experiences of how they are handling today's sanctions and enforcement challenges.

The US's May 2018 exit from the Joint Comprehensive Plan of Action ('JCPOA') and the subsequent re-imposition of nuclear sanctions against Iran – counterposed with the EU's

response, underscoring the value of the JCPOA – coupled with the targeting of high-net-worth Russians under the Countering America's Adversaries Through Sanctions Act ('CAATSA'), have created a good slab of work for compliance professionals in global enterprises.

Other measures to have had an

impact – the extent of which, naturally depends on where the business is focused geographically – include the upscale in sanctions against Venezuela and Nicaragua on humanitarian grounds and continued sanctions against North Korea and Cuba.

Iran: split headache

The need for a swift untangling of any business with Iran has kept compliance professionals busy over the past year. ‘Three different batches of US sanctions on Iran have been re-imposed, and the goalposts keep on being moved. It is difficult to keep track,’ comments a compliance professional in an international logistics company with operations in Dubai, a business centre which has close links to Russia, Syria and Iran.

All of the compliance professionals we spoke to were in consensus that the divergence between the US and the EU on Iran had caused major challenges in maintaining compliance. ‘This remains a sensitive issue to manage,’ said one working in the oil and gas services sector. ‘Practical blocking issues relating to payments and lack of insurance become the drivers.’

Despite the determination of the EU and its JCPOA partners to keep the 2015 deal alive, it is ultimately the banks financing world trade that call the shots, and they will not risk losing their ability to clear foreign money transactions into all-important US dollars: ‘Fear of the US regulator looms large, not just in terms of sanctions but also the risk of reputational damage, so banks err on the side of caution,’ says a professional working in sanctions compliance support. Indeed, the conservative stance of banks and insurers in evaluating which deals they will participate in often exceeds that required by the regulators.

The Trump administration has so far exhibited a predilection for secondary sanctions – which constitute a key plank of its ‘maximum pressure’ campaign against Iran. A recent report by the European Council on Foreign Relations (‘ECFR’) identifies US secondary sanctions and its ‘aggressive economic statecraft’ as ‘a critical challenge’ for Europe, with the risk that in future states will ‘weaponise’ economic interdependence with the EU to target countries that are more important to the EU economy than Iran, such as China or Russia. The report argues that the EU and its

Everyday sanctions headaches

WorldECR canvassed the views of trade compliance professionals as to what they saw as key and regular sanctions-related challenges arising today. In no particular order, they identified the following:

- Sanctions impacting beyond the traditional industry targets of banking and energy
- Aggressive expansion of US extraterritorial regulatory ambitions
- Inconsistency among regimes in selection of parties for designation
- Rock and hard place dilemma over US vs EU regulation
- Uncertainty arising as sanctions are used as tools for trade negotiation
- Global supply chains bring tougher screening challenges

Member States should strengthen sanctions policy, ‘build up their deterrence and resilience to secondary sanctions, and prepare to adopt asymmetric countermeasures against any country that harms European interests through secondary sanctions.’

The EU has already attempted to ‘push back’ against the US’s stance with its own blocking regulation. This piece of legislation – originally conceived in 1996 to counter the US’s unilateral sanctions on Cuba and other countries – was reactivated in 2018, adding US sanctions on Iran to the list of

mechanism a legitimate target for sanctions.

The prospect of an extended standoff between the EU and US on the direction and use of sanctions, as foreseen in the ECFR’s report, will inevitably cause more uncertainty for global businesses juggling distinct sanctions regimes. The dilemma in which European companies trading with Iran find themselves has been compounded by the US Department of the Treasury’s Office of Foreign Assets Control (‘OFAC’) new guidelines (‘A Framework for OFAC Compliance Commitments’), released in May. These outline what OFAC expects from companies in terms of compliance and give an indication of OFAC’s proposed enforcement strategy. Although the guidelines do not specifically relate to Iran, they have a bearing on the situation. OFAC advises companies to develop five ‘essential components’ in their sanctions compliance programmes: commitment from management, risk assessment, internal controls, testing and auditing, and training.

Although a welcome insight into OFAC’s workings, OFAC’s expectations place EU-based companies in something of a bind: a formal compliance programme tailored to OFAC’s guidelines could be used as evidence that the company intended to comply with US sanctions on Iran, when this is expressly prohibited by the EU’s blocking regulation.

Although enforcement penalties



‘For the past four or five years OFAC’s primary target has been the banks. That has changed. Now banks, owners, operators, insurers are all vulnerable across a range of business sectors. The whole supply chain is being targeted.’

extraterritorial rules which EU entities are prohibited from following.

The EU signatories to the JCPOA, France, Germany and the UK, have put in place an SPV, INSTEX, which seeks to allow companies to bypass using an Iranian institution, the Iranian rial or US dollars in transactions with Iran. However, it seems few people have great expectations for the SPV, particularly as the US has already intimated that it would consider the




vary between EU Member States, the potential consequence of ignoring the EU’s blocking regulation ranges from fines of up to €500,000 and a possible three-year prison sentence in Ireland, to a €60,000 fine in Spain, and an unlimited fine in the UK.

The long arm of the law

It is not just fear of contravening the black-and-white letter of US sanctions law (or guidance) that keeps

sanctions-intelligence.com

The sanctions environment remains dynamic in the second quarter 2019:

Quarterly Sanctions Statistics 2nd Quarter 2019 (Apr 01 - Jun 30) www.sanctions-intelligence.com	 US OFAC SDN	 EU Consolidated	 UN Consolidated	Σ Total
Number of entries (June 30 2019)	7.725	2.109	1.020	12.989
Amendments				
Added entries	199	3	2	204
Changed entries	18	155	685	858
Changed entries	-	-	482	482
Removed entries	1	56	60	117
Amendments total	217	214	1.229	1.661

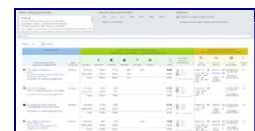
Extract from quarterly sanctions analysis. See webpage for further details and methodology.

A central question for every sanctions professional:
How to stay on top of frequently changing sanctions issues?
And where to find relevant information?

Sanctions-intelligence.com helps with answers:

A directory of sanctions lists and their characteristics

- Knowledge database of numerous sanctions lists/programs
- Accessibility, formats, search options and much more
- Updated on a regular basis



Global List Profiles

Information on daily sanctions list updates

- Updates of US OFAC SDN, EU, UK and UN Sanctions Lists
- Chronology of recent sanctions list changes
- Delta comparison tool with details on entry level



Daily Sanctions Updates

Analyses and trends for risk assessments

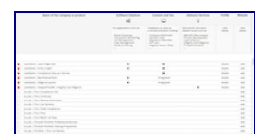
- Weekly/monthly/quarterly and topical reviews
- Analysis of indicators (frequencies, programs, countries etc.)
- Newsletter/Alerts on recent changes



News and analyses

Overview where to find help if needed

- Listing of sanctions-related commercial offerings
- Software products, data/list vendors, advisory services etc.



Service Providers and Tools

<https://www.sanctions-intelligence.com/subscription>

international compliance professionals on their guard, but the endless scope of potential targets for OFAC.

‘For the past four or five years OFAC’s primary target has been the banks,’ says the sanctions compliance support professional. ‘That has changed. Now banks, owners, operators, insurers are all vulnerable across a range of business sectors. The whole supply chain is being targeted.’

Russia sanctions: CAATSA

In April 2018 the Trump administration imposed new sanctions under CAATSA on seven Russian oligarchs and 12 companies they owned or controlled, as well as 17 senior Russian government officials, state-owned Russian weapons trading company Rosoboroneksport, and its subsidiary, Russian Financial Corporation Bank. The designations meant heightened screening obligations related to ‘know your customer’ needed to be put in place – not easy when the designated Russian oligarchs and their companies are enmeshed in a web of business relationships around the world, creating serious compliance challenges for businesses active in the same spheres of interest. Oleg Deripaska, for example, not only owned RUSAL, GAZ Group and EuroSibEnergo but has a stake in construction companies, agricultural companies and an aviation business that runs three large airports in Russia.

‘Due to the complexity of the situation systemised screening cannot be relied upon,’ says one compliance professional. ‘The technical and industry-specific nature of the due diligence related to “prohibited” activities also adds complications, as this cannot be undertaken by third parties, such as banks and insurers.’

OFAC’s 50% rule is also ‘causing an inordinate amount of angst,’ according to a US-based compliance professional working in a global IT and business processes company. ‘It is so difficult to find the real owners; as there are so many shell companies and information in other languages etc. While the 50% rule has always been in place, it seems like the US government has relied on it a lot more (read “enforced”) after the Russian sanctions, and the oligarchs are pretty smart at covering their tracks.’

The 50% rule indicates how OFAC

Can automated compliance screening close the gap and minimise compliance errors?

Automated compliance screening is widely viewed as a useful tool for identifying designated parties or raising possible red flags for further investigation or due diligence.

‘Automated compliance screening needs to be adaptable and configurable to the individual business’s own level of risk,’ says a professional working in sanctions compliance support. ‘The automated process should aim for minimum human error, and minimum human input.’

He points out that it is important for any compliance system to keep pace with the

regulatory landscape – in line with the much-cited truism that there is a change in global financial regulation every 12 minutes – and that automated compliance screening can do that.



Others are sceptical: ‘Compliance screening cannot always keep up with developments from an automation point of view,’ says an oil and gas services compliance professional. ‘We are reliant on the human factor; good knowledge and required reflexes.

These take time to develop, effort to maintain, and yet still [screening] may ultimately fail because of it.’

determines whether companies not appearing on the SDN List are blocked; they may be blocked if owned by other companies or individuals who do appear on the list. ‘My personal opinion is that if OFAC doesn’t want us to do business with certain entities, OFAC should tell us who those entities are,’ this compliance professional says.

The difficulties inherent in meeting compliance obligations where Russian entities are concerned are a common theme, such as in the case of the company with a global, high-volume logistics operation: ‘There have been instances concerning the Russia sanctions where we have been unaware that there was a suspect party in the transaction, as the due diligence did not show up any red flags,’ says a compliance professional in the sector.

Another frustration is that the EU, the US and Canada have not imposed sanctions on the same Russian oligarchs. ‘A few individuals may be the same, but otherwise, if you are a global company, it can be a challenge, especially when a country exercises its law extraterritorially,’ says a seasoned US-based compliance professional.

Lack of uniformity in global sanctions (Iran, Russia as cases in point) is not only ‘a compliance challenge’ but arguably weakens their effectiveness. Cuba is another stumbling block – as both the EU’s blocking regulation and Canada’s laws prohibit compliance with US sanctions on Cuba. As Canadian sanctions specialists point out, compliance with

US sanctions alone – as the most potent global protagonist – can trip you up, if you assume that Canada and its allies take the same position.

Are the regulators doing enough?

Opinion is divided as to whether the regulators – in particular OFAC – are doing enough to aid businesses with the fast-changing world of sanctions compliance. ‘OFAC releases FAQs, but the answers fall short of the different scenarios that may or may not be anticipated,’ says one compliance professional.

‘I believe that the guidance is clear in terms of “What” – but the “How” is left to each company. No doubt many wheel re-inventions are the consequence,’ says another.

Others find OFAC under-resourced and report that it is difficult to obtain guidance information. ‘If you call, they generally tell you to submit a licence application for guidance,’ says one. ‘But OFAC doesn’t have many people reviewing licences and it can take months and even years to get anything back. OFAC needs to provide more resources and more training.’

Other tailor-made concerns

Each industry sector will have its own compliance headaches. The GDPR obligations on safeguarding data and ‘right to be forgotten’ have thrown up some challenges for businesses with an EU nexus: ‘Not so much with customer data where the new legislation has been anticipated, but with HR systems,

“Extremely intelligent and strategically astute...
Outstanding at handling economic sanctions/export
control matters, both from a contentious and
non-contentious perspective.”

– TESTIMONIAL IN *LEGAL 500*

- ▶ One of Washington’s go-to firms for export controls and sanctions enforcement defense.
- ▶ Our Economic Sanctions and Export Controls practice is led by a former Department of Justice official in the National Security Division and the Chair of our highly-ranked White Collar Practice.
- ▶ We have decades of experience interacting with government enforcement officials, from line-level enforcement staff through to the Department of Justice leadership.
- ▶ We use an integrated “team approach,” working closely with highly-ranked international investigations and compliance lawyers in the anti-corruption, white collar, and anti-money laundering spaces.
- ▶ International Trade and Investigations lawyers individually ranked in both *Chambers* and *Legal 500*
- ▶ 2018 *Global Investigations Review*: GIR Top 30 Global Investigations Practice, 2016 Boutique or Regional Practice of the Year
- ▶ Ranked in 2019 *Chambers* Global, USA, and Latin America: Corporate Investigations (Global-wide and Latin America-wide), FCPA (United States), Corporate Crime & Investigations (United States), and Litigation: White Collar Crime & Government Investigations (District of Columbia)
- ▶ Ranked in 2019 *Legal 500*: International Trade (United States)

Miller & Chevalier

where information on who has applied for which job is stored. Who has access is a challenge,' says one compliance professional.

The deterioration of relations between China and the US and resulting trade tariffs have not yet had a direct impact on the global operations of the businesses we spoke to, but

customers are reportedly making changes to their supply chains to source components such as steel or telecommunications equipment from outside of China.

And although there are no trade compliance consequences, there are practical 'bottom line' implications in terms of tariffs driving price increases

in IT equipment, for example.

Looking ahead, with further targeted US sanctions against Russia and Iran a distinct possibility, and Iran threatening to overturn its commitments under the JCPOA, global compliance professionals across business sectors have plenty to handle right now. ■

THE WORLDEC EXPORT CONTROLS AND SANCTIONS FORUM 2019



LONDON: 3-4 OCTOBER

DC: 15-16 OCTOBER

VISIT WWW.WORLDEC.COM/CONFERENCE-2019/ FOR DETAILS

official sponsors

**Debevoise
& Plimpton**

**Hogan
Lovells**

BakerHostetler

GW Graf von Westphalen

Miller & Chevalier

KPMG

F T I
CONSULTING

WHITE & CASE

OFAC clarifies its compliance expectations

By Satish M. Kini and David G. Sewell

On 2 May 2019, the US Office of Foreign Assets Control ('OFAC') published 'A Framework for OFAC Compliance Commitments' (the 'SCP Guidance'), comprehensive guidance on its expectations for sanctions compliance programmes ('SCPs'). The SCP Guidance follows several enforcement settlements OFAC used to offer targeted guidance regarding the shortfalls of companies' SCPs. Taken together, the SCP Guidance and settlements offer the most detailed statements to date of OFAC's views on what constitutes an effective programme to comply with US sanctions requirements.

The SCP Guidance

The SCP Guidance reiterates OFAC's policy that an appropriate SCP should be 'risk based' and tailored to account for factors such as 'the company's size and sophistication, products and services, customers and counterparties, and geographic locations'. Notwithstanding any tailoring, OFAC describes five 'essential' components for every SCP:

- **Management commitment:** Involvement by senior management, adequate resourcing and promotion of a 'culture of compliance' that rewards prudent conduct and permits escalation of potential issues 'without fear of reprisal';
- **Risk assessment:** Ongoing, periodic review of the company's clients, products, services and geographic locations, among other risk factors, to identify areas in which the company may encounter compliance obligations;
- **Internal controls:** Written policies and procedures that clearly and effectively identify, interdict, report and mitigate non-compliant activity;
- **Testing and auditing:** Independent assessment of the effectiveness of internal controls and checks for inconsistencies with operations; and
- **Training:** Periodic training, at least annually, that provides appropriate employees and other stakeholders job-specific knowledge regarding their sanctions compliance responsibilities.

Root causes

The SCP Guidance also addresses 'root causes' of compliance failures and describes deficiencies OFAC has identified repeatedly in enforcement actions. The SCP Guidance identifies 10 key 'root causes':

- lack of a formal OFAC SCP;
- misinterpreting, or failing to understand the applicability of, OFAC's regulations;
- facilitating transactions by non-US persons (including through or by overseas subsidiaries or affiliates);
- exporting or re-exporting US-origin goods, technology or services to sanctioned persons or countries;
- utilising the US financial system, or processing of payments to or through US financial institutions, for commercial transactions involving OFAC-sanctioned persons or countries;
- sanctions screening software or filter faults;
- improper due diligence on customers/clients (e.g., ownership, business dealings);
- decentralised compliance functions and inconsistent application of an SCP;
- utilising non-standard payment or commercial practices; and
- individual liability.

Enforcement action lessons

In recent months, OFAC has begun including in enforcement notices summaries highlighting certain compliance practices that OFAC believes relevant. Two key themes emerge from those actions.

Cross-border M&A: Four recent enforcement actions involve variations on the following fact pattern. A US-based company acquires a non-US subsidiary. In the course of the acquirer's due diligence, it discovers that the foreign company does business in Cuba or Iran, both subject to a US embargo. The holding company takes steps to fold the company, once acquired, into its SCP and prevent the new non-US subsidiary from doing such prohibited business. Nonetheless, the subsidiary continues to do such business anyway.¹

These actions demonstrate that heightened pre-acquisition due diligence does not suffice to ensure post-acquisition sanctions compliance. They also show the importance of a robust system of internal

Links and notes

¹ https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190207_kollmorgen.pdf; https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190327_decker.pdf.

² https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190214_applichem.pdf

³ https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190131_elf.pdf

controls that allows a company to respond decisively to sanctions violations once discovered. In one example, a US company repeatedly received notice that its foreign subsidiary was engaging in sales to Cuba.² The acquirer responded by reinforcing to subsidiary management that such sales must cease, securing representations from them to that effect and even disclosing the initial compliance failure to OFAC. The company failed, however, to stop the subsidiary's sales and ultimately was penalised \$5.5 million.

International supply chains: In two other recent OFAC enforcement actions, US companies unwittingly purchased goods sourced from sanctioned jurisdictions through suppliers based in nearby countries that represented that the goods were compliant with US legal restrictions.³

These cases evidence the importance of supply chain due diligence. OFAC considers international trade to be a high-risk activity and expects suppliers operating near sanctioned countries to adopt and abide by compliance procedures commensurate with such risk.

Conclusion

Armed with OFAC's expectations, US firms and international businesses doing business with a US nexus should review and update their SCPs to meet OFAC's baseline expectations. Doing so may lessen the risk of US sanctions violations and could reduce the potential liability should an apparent sanctions violation occur. ■



Satish M. Kini (Washington, D.C.) is a partner and David G. Sewell (New York) is counsel in the Financial Institutions Group at Debevoise & Plimpton LLP.

www.debevoise.com

Helms-Burton litigation adds a wrinkle to business ventures in Cuba

By Cari N. Stinebower and Christopher B. Monahan

On 2 May 2019, in an effort to ratchet up sanctions pressure on Cuba for supporting the Maduro regime in Venezuela, the Trump administration announced it was not renewing a waiver to the controversial Title III of the Cuban Liberty and Democratic Solidarity Act of 1996 (Helms-Burton Act, Pub.L. 104-114, 110 Stat. 785, 22 U.S.C. §§ 6021-6091). Title III provides a right of action for US citizens to file lawsuits in US federal courts seeking damages from businesses that ‘traffic’ in property that was seized by the Cuban government during the Cuban revolution. It is making news in 2019 because Mr. Trump is the first president not to waive Title III since its enactment in 1996.

The law has been controversial – and Democratic and Republican administrations alike have waived it since 1996 – because, unlike most traditional sanctions, in an effort to strengthen sanctions pressure on the Cuban government, Title III targets businesses outside Cuba. At the time of its passage, the thought was that the target of any litigation would be non-US businesses (because there was almost no trade between Cuba and the United States). The world took immediate notice: the EU filed a complaint in the World Trade Organization and enacted ‘blocking’ legislation that prohibited EU Member States from complying with the Act. Mexico and Canada put similar laws in place.

At first blush, the law may seem sensible because it allows for legal redress for persons whose property was expropriated without compensation. That said, it has drawn significant criticism – and not only because it would allow suits against US and non-US companies for conducting entirely lawful business. In many critics’ view, much of the likely litigation under Title III constitutes an inappropriate challenge to Cuban

sovereignty. That is because, in a number of plausible (if not likely) scenarios under Title III, a US person can bring a cause of action based on (1) the Cuban government’s taking of a Cuban citizen’s property and then (2) a third-country entity’s ‘trafficking’ in that property. US courts would be sitting in judgement of the sovereign acts of other countries’ governments – i.e., the Cuban

It has drawn significant criticism – it would allow suits against US and non-US companies for conducting entirely lawful business.

government’s taking of property and those third-country trading partners from which the defendants hail. In 2019, it also means that a suit can be brought against a US entity whose dealings in Cuba were pursuant to a Department of the Treasury- or Commerce-issued licence.

Despite the historic controversy, the litigation has begun and likely will continue with gathering intensity. The cause of action is novel and this promises to be an interesting year. For starters, it is not clear how judges will respond to certain arguments. For example, entities operating in Cuba under US government authorisations are not exempt from litigation. In addition, there does not appear to be an affirmative defence for a business providing humanitarian goods under a US Commerce or Treasury Department authorisation if that business was ‘trafficking’ in expropriated property in carrying out that licensed activity.

Claimants also are challenging activity that appears to be exempt from these claims. The first suit brought was against

a US company, Carnival, for its alleged trafficking in expropriated property by virtue of its use of a Cuban port. Not only was Carnival’s activity at the port authorised by the US and Cuban governments, Title I of Helms-Burton explicitly exempts from the definition of ‘trafficking’ transactions ordinarily incident to lawful travel. Carnival has filed a motion to dismiss partially on this basis, but potential litigants and defendants alike will watch how the court rules.

In addition to the Carnival case, plaintiffs filed a series of cases claiming their interest in the San Carlos Hotel is being trafficked by the booking website, Trivago. Again, this case appears to call into question whether trafficking will include transactions incident to travel – and will likely help to better define the parameters of that exemption. How the courts rule may open up numerous cases against the various hotel properties in Cuba. This case also is interesting because plaintiffs are claiming that the booking website is trading in the hotel’s historic reputation as well as the physical property, which may be their key to outmanoeuvring the travel exemption defence. If successful, one can expect to see other claimants employing similar tactics to bring traditional travel service providers into the crosshairs of this litigation. Other cases are likely to arise relating to other hotel chains operating in Cuba – which likely will raise complex jurisdictional questions and may lead to lengthy discovery.

In addition to novel legal questions, this will be an interesting year for litigants to observe the response of the EU, Mexico, and Canada, which have forms of blocking statutes in place. The EU’s public response has been strong. EU Member States have pledged that they will protect EU entities who are facing Title III cases. In addition, it appears that the EU blocking law will preclude law firms with offices in the US and EU from acting as plaintiff’s counsel because the blocking statute can be used against the EU lawyers of those firms.

We are watching all of the pending litigation and even some we anticipate that has not yet been filed. We are also advising clients that might be the subject of this litigation on the best way to prepare to defend claims under Title III. ■



Cari N. Stinebower and Christopher B. Monahan are partners at Winston & Strawn LLP, based in the firm’s Washington, DC office.

www.winston.com

Four important lessons from recent US export controls and sanctions enforcement actions

By Brian J. Fleming and Timothy P. O'Toole

At least a few times every month, the US Department of Commerce's Bureau of Industry and Security ('BIS') and the US Department of the Treasury's Office of Foreign Assets Control ('OFAC') announce the issuance of new civil monetary penalties and explain the basis for these penalties. These announcements are very important: Studied carefully, they can help companies spot, remediate, and potentially prevent serious consequences. We discuss below four specific lessons that companies can learn from reviewing these recent enforcement actions.

Identifying US touchpoints is key

Probably the most important challenge for any company is identifying when US law applies. Recent enforcement actions have involved situations where non-US companies, or foreign subsidiaries of US companies, mistakenly thought that US sanctions or export control laws did not apply but were wrong – meaning that their dealings with specially designated nationals ('SDNs') did in fact violate US law, (Zoltek Companies and Cobham Holdings), as did their purchase of Iranian supply chain products (ZAG IP, LLC).

The highest priority enforcement actions, moreover, have involved a related issue in which US jurisdiction continued to apply despite the seemingly foreign nature of the transaction. These enforcement actions included the re-export to Iran of US-origin oilfield products (Yantai Jereh), the export to Iran of consumer goods (Stanley Black and Decker), and consumer services (Kollmorgen) by US-owned foreign subsidiaries.

The basic lesson of these cases is that foreign companies and foreign subsidiaries of US companies must carefully monitor their US touchpoints so as to accurately assess and comply with their obligations under US law. The failure to do so can result in very serious consequences.

The M&A process creates extra risk and requires extra care

Another lesson arising from recent enforcement actions involves the merger and acquisition process. When a US company acquires a foreign company, US export controls and sanctions laws often apply to the target company after the

purchase. The purpose of the due diligence process is both to identify these risks and to effectively address them. This latter point is key: New export controls and sanctions issues arising from the purchase must be fixed as soon as possible. Indeed, three very recent enforcement actions (Stanley Black and Decker, Kollmorgen, and AppliChem) involve scenarios in which the US parent

Companies must take proactive steps to the mitigate significant sanctions risk arising from global supply chains, especially in high-risk regions.

identified potential sanctions problems as part of the pre-acquisition due diligence process but did not put into place procedures and personnel sufficient to remediate those issues post-closing.

Know your supply chain

Another lesson from recent enforcement actions involves supply chain management. In January of this year, OFAC imposed a penalty on e.l.f. Cosmetics ('ELF') for importing false eyelash kits into the United States because the kits contained materials from North Korea. The kits had come from ELF's Chinese supplier and there was no evidence ELF had any knowledge that some of the materials in the kits were of North Korean origin. Nonetheless, OFAC faulted ELF for its lack of a sanctions compliance process focused on its supply chain, announcing that 'this enforcement action highlights the risks for companies that do not conduct full-spectrum supply chain due diligence when sourcing products from overseas, particularly in a

region in which the DPRK, as well as other comprehensively sanctioned countries or regions, is known to export goods.'

OFAC then encouraged companies to mitigate such risks by 'implementing supply chain audits with country-of-origin verification; conducting mandatory OFAC sanctions training for suppliers; and routinely and frequently performing audits of suppliers.'

The ELF enforcement action is a wake-up call that tells all US companies that they must take pro-active steps to the mitigate significant sanctions risk arising from global supply chains, especially in high-risk regions. The failure to do so – even when the US company has no knowledge of sanctioned goods in its supply chain – can result in significant penalties.

When a problem is spotted, it must be addressed

The final lesson is more basic, but it is probably the most important of all: When a company identifies a sanctions or export control issue, it must address it. Indeed, the largest penalties are generally reserved for those enforcement actions (such as ZTE, Societe Generale, Huawei, Kollmorgen, and AppliChem, etc.) where a company spots a potential US enforcement issue but then does nothing to fix the problem. Even worse, the companies in some of these cases were alleged to have affirmatively concealed sanctions issues in the hope that US regulators would not discover them.

This head-in-the-sand (or even worse shovel-in-the-sand) approach is where we see the biggest penalties. This is not to say that every issue must be voluntarily disclosed to regulators – that is often a far different and more complex question. But what is clear in every case is that when a sanctions or export control issue arises, the problem must be confronted and quickly remediated. ■



Brian Fleming and Timothy O'Toole are members of D.C.-based law firm Miller & Chevalier Chartered.

www.millerchevalier.com

WorldECR

The journal of export controls and sanctions

Contributors in this issue

William M. LeoGrande, American University

Jasper Helder, Chiara Klau, Daniel Lund and Isabel Foster, Akin Gump
www.akingump.com

Tim Hesselink, Marc Padberg, Eline Mooring and Ton Bendermacher, Kneppelhout & Korthals N.V.
www.kneppelhout.nl

Stuart Simons and Sujitra Sukpanich, Deloitte Thailand
www.deloitte.com

Steven Brotherton and Amie Ahanchian, KPMG LLP
www.KPMG.com

WorldECR Editorial Board

Michael Burton, Jacobson Burton Kelley PLLC
mburton@jacobsonburton.com

Jay Nash, Nash Global Trade Services
jaynash@gmail.com

Dr. Bärbel Sachs, Noerr, Berlin
baerbel.sachs@noerr.com

George Tan, Global Trade Security Consulting, Singapore
georgetansc@sg-gtsc.com

Richard Tauwhare, Richard Tauwhare Consulting Ltd
richard@rtclimited.com

Stacey Winters, Deloitte, London
swinters@deloitte.com

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

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

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

WorldECR is published by D.C. Houghton Ltd.

Information in WorldECR is not to be considered legal advice. Opinions expressed within WorldECR are not to be considered official expressions of the publisher. The publisher assumes no responsibility for errors and omissions appearing within. The publisher reserves the right to accept or reject all editorial and advertising matter. The publisher does not assume any liability for unsolicited manuscripts, photographs, or artwork.

***Single or multi-site: Do you have the correct subscription?** A single-site subscription provides WorldECR to employees of the subscribing organisation within one geographic location or office. A multi-site subscription provides WorldECR to employees of the subscribing organisation within more than one geographic location or office. Please note: both subscription options provide multiple copies of WorldECR for employees of the subscriber organisation (in one or more office as appropriate) but do not permit copying or distribution of the publication to non-employees of the subscribing organisation without the permission of the publisher. For full subscription terms and conditions, visit <http://www.worlddecr.com/terms-conditions>

For further information or to change your subscription type, please contact Mark Cusick - mark.cusick@worlddecr.com

© D.C. Houghton Ltd 2019. All rights reserved. Reproduction in whole or in part of any text, photograph, or illustration without express written permission of the publisher is strictly prohibited.

ISSN 2046-4797. Refer to this issue as: WorldECR [0081]

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 81. JULY/AUGUST 2019
www.WorldECR.com