International Comparative Legal Guides

Sanctions 2020

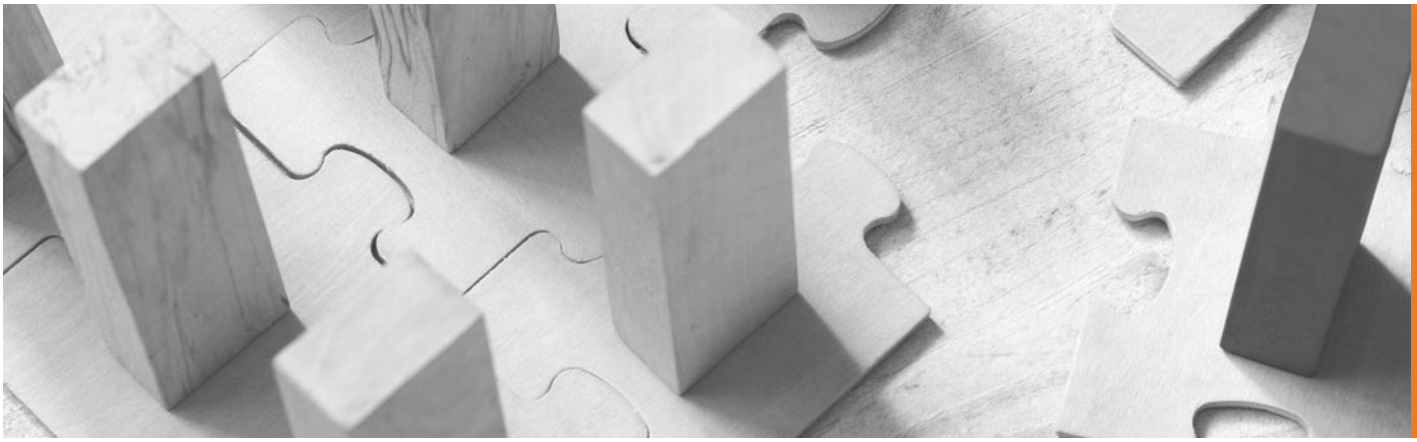
A practical cross-border insight into sanctions law

First Edition

Featuring contributions from:

Allen & Gledhill LLP
BonelliErede
Bonifassi Avocats
BSA Ahmad Bin Hezeem & Associates LLP
De Brauw Blackstone Westbroek N.V.
DELTA legal
Dentons US LLP
Djingov, Gouginski, Kyutchukov & Velichkov
DORDA Rechtsanwälte GmbH
Esenyel & Partners
Eversheds Sutherland
Hill Dickinson LLP
Homburger
JSA
JunHe Law Offices
Kluge
Lee & Ko
Linklaters LLP
Miller & Chevalier
MinterEllison
Navigant Consulting, Inc.
Nishimura & Asahi
Noerr LLP
Paul, Weiss, Rifkind, Wharton & Garrison LLP
Plesner
Proskauer Rose LLP
Stikeman Elliott LLP

ICLG.com



ISBN 978-1-83918-003-3
ISSN 2633-1365

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Publisher
Jon Martin

Senior Editors
Caroline Oakley
Rachel Williams

Sub-Editor
Amy Norton

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Sanctions 2020

First Edition

Contributing Editors:
Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Strategic Partners

Expert Chapters

Country Q&A Chapters

Sanctions and Export Controls Enforcement Trends


Timothy P. O'Toole


Aiysha S. Hussain

Miller & Chevalier

Introduction

With the U.S. government's prolific activity in the sanctions and export spheres, this year has seen some significant overarching trends implicating sanctions and export compliance. Specifically, U.S. agencies – including the Office of Foreign Assets Control ("OFAC"), the Bureau of Industry and Security ("BIS"), the Department of Justice ("DOJ"), and state law enforcement agencies – are coordinating efforts in sanctions and export enforcement and are acutely focused on issues relating to Iran, Cuba, Venezuela, and China.

The U.S. government's increasingly aggressive stance against Iran and Cuba is reflected in OFAC's 2019 enforcement actions. With respect to Iran, in 2018 the Trump administration withdrew from the Joint Comprehensive Plan of Action ("JCPOA") and reimposed secondary sanctions targeting key sectors of the Iranian economy. As a result, since the U.S.'s withdrawal, the Trump administration has been vigourously pursuing sanctions against Iran. As for Cuba, the Trump administration has rolled back Obama-era policies that loosened restrictions on travel to Cuba. Most recently, citing Cuba's destabilising role in Venezuela and Nicaragua, the U.S. government ended authorisation of group people-to-people educational travel.[1] OFAC civil-penalty enforcement actions for violations of sanctions against Iran and Cuba dominate the 2019 track record, with six out of 16 actions that involved violations of Iranian sanctions and seven out of 16 actions that involved violations of Cuban sanctions. The Trump administration's aggressive posture towards Iran and Cuba is likely to continue beyond 2019.

The U.S. government also continued to expand sanctions against Venezuela as tensions escalate under Nicolás Maduro's leadership. Currently, the U.S. Department of Treasury has sanctioned 129 individuals, designated Venezuela's state oil company ("Petróleos de Venezuela, S.A." or "PdVSA"), gold industry, central bank, and other entities. Most recently, President Trump issued Executive Order 13884 blocking the property interests of the Maduro government, prohibiting U.S. persons from engaging in transactions with the Maduro government, and permitting secondary sanctions on non-U.S. persons that assist or support the Maduro government. As there are no signs of the conflict in Venezuela subsiding, Venezuela is likely to remain a key U.S. sanctions target.

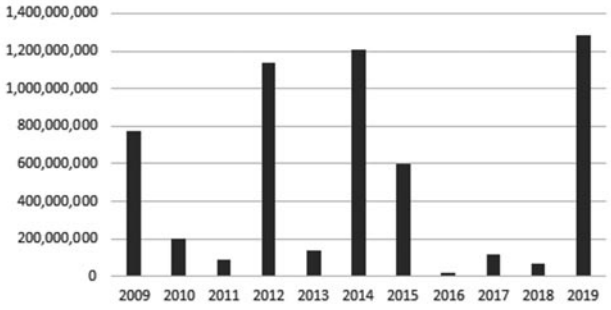
From a primarily export controls perspective, China is a central focus of the United States because of its acquisition of sensitive technologies and intellectual property from the United States, particularly by Chinese government players, and its trade relationship with North Korea. It appears that the U.S. government is leveraging numerous government agencies, including law enforcement and regulatory tools, to advance U.S. national security interests to increase pressure on China. To date, included in this wholesale push are the DOJ and BIS's enforcement tools. Given the U.S. government's concerns that China is misappropriating U.S. technology and intellectual property and China's continued trade relationship with North Korea, this trend is also likely to persist long after 2019.

These larger policy-based trends inform sub trends that we discuss below. This chapter proceeds as follows: (1) the first section discusses enforcement trends stemming from OFAC's 2019 enforcement actions and the practical effects of OFAC's recent publication of its "Framework for OFAC Compliance Commitments" ("Compliance Framework" or "Framework"); and (2) the second section discusses key export controls enforcement trends that involve the DOJ and BIS, seriously impacting U.S. business with certain key China-based companies.

OFAC's 2019 Civil Penalty Total is the Largest in the Last 10 Years

The year 2019 witnessed a substantial increase in OFAC civil-penalty enforcement actions compared to the last four years. Year to date, OFAC has imposed $1,281,394,219 in penalties, which is significantly higher than years past and the highest total amount in the last 10 years.

10-Year Snapshot of OFAC Penalties



Although a large portion of the total penalty amount is divided between UniCredit Bank with $611,023,421 and Standard Chartered Bank with $657,040,033, most enforcement actions in 2019 did not involve banks but a variety of companies in different industries, such as engineering, manufacturing, and shipping. These actions indicate that OFAC is expanding its scope beyond banking and finance actors and targeting a variety of different industries, which means that companies should not presume that their business in a non-banking industry might insulate them from OFAC's attention. Some notable trends from the 2019 OFAC enforcement actions that we discuss below are OFAC's focus on sanctions violations of U.S. foreign subsidiaries and sanctions violations emanating from supply chain weaknesses. Both trends, and OFAC's issuance of its Compliance Framework, indicate that companies should take a proactive approach in implementing robust compliance programmes and stay abreast of the continually evolving sanctions and export policies.

Recent OFAC Enforcement Actions Demonstrate the Importance of Comprehensive M&A Due Diligence, Follow-up Sanctions Training, and Compliance Audits

Enforcement actions against Kollmorgen Corporation ("Kollmorgen"), AppliChem GmbH ("AppliChem"), Stanley Black and Decker ("Black & Decker"), and Expedia Group, Inc. ("Expedia") reflect the sanctions compliance risk companies face when integrating new acquisitions. When the U.S.-based companies Kollmorgen, Illinois Tool Works, Inc. ("ITW"), and Black & Decker acquired the foreign companies at issue, each was aware the respective subsidiaries had previously engaged in transactions with countries subject to U.S. economic trade sanctions, and implemented varying measures to prevent violations. Despite this, the foreign subsidiaries continued to engage in prohibited operations. OFAC considered the companies' efforts to prevent sanctions violations, but because OFAC takes a strict liability approach to sanctions violations, these measures did not necessarily insulate the companies from an OFAC enforcement action. We discuss each case below.

- Kollmorgen: Kollmorgen acquired control of a Turkish company, Elsim Elektroteknik Sistemler Sanayi ve Ticaret Anonim Sirketi ("Elsim"), in 2013. During acquisition due diligence, Kollmorgen learned that Elsim had a customer base in Iran with which it had been conducting business. As a result, Kollmorgen implemented a range of pre- and post-acquisition compliance measures to ensure Elsim complied with U.S. sanctions. Kollmorgen discovered the violations through an Elsim employee's complaint via the ethics hotline. Kollmorgen conducted an internal investigation and filed a voluntary self-disclosure with OFAC. OFAC fined Kollmorgen $13,381 and determined this to be a non-egregious case, in part because of Kollmorgen's extensive compliance efforts and voluntary self-disclosure.
- AppliChem: ITW acquired AppliChem, a German company that manufactures chemical and reagents for the pharmaceutical and chemical industries. During acquisition negotiations, ITW discovered references to countries subject to U.S. economic and trade sanctions on AppliChem's website. ITW advised AppliChem that it would need to cease all Cuba transactions after the acquisition. Notwithstanding this, AppliChem continued to collect on existing orders with Cuban nationals under pre-acquisition contracts. In 2013, ITW submitted a voluntary self-disclosure to OFAC regarding these collections. In 2015, OFAC issued a cautionary letter to ITW in response. Thereafter, in 2016, an anonymous report through an ITW ethics helpline indicated that AppliChem continued to make sales to Cuba. ITW investigated the matter and discovered that AppliChem designed a scheme to conceal transactions with Cuba by referring to them in code word, meaning no documents mentioned the word Cuba. OFAC determined this was an egregious case and assessed a civil monetary penalty of $5,512,564 against AppliChem.
- Black & Decker: Black & Decker acquired its subsidiary in China, Jiangsu Guoqiang Tools Co. Ltd. ("GQ") in 2011. During acquisition due diligence, Black & Decker learned that GQ exported to Iran. Black & Decker required GQ to cease sales to Iran and had senior management certify they would not sell to Iran. After acquisition, Black & Decker provided a series of training on U.S. sanctions and the Foreign Corrupt Practices Act to the subsidiary's employees. Black & Decker, however, failed to implement procedures to monitor and audit GQ's operations.

  Despite knowing this violated corporate polices and U.S. sanctions, GQ continued making sales to Iran for two years and covered up evidence of such transactions. Although Black & Decker voluntarily disclosed the matter, OFAC determined this was an egregious case and fined Black & Decker $1,869,144.
- Expedia: Expedia's foreign subsidiaries dealt in property and interests in property of Cuba or Cuban nationals by assisting 2,221 persons, some of whom were Cuban nationals, with travel-related services for travel within Cuba or between Cuba and locations outside the United States. These violations of the Cuban Assets Control Regulations occurred because certain Expedia foreign subsidiaries lacked an understanding of the U.S. economic sanctions laws. With respect to one foreign subsidiary, Expedia failed to inform the subsidiary until 15 months after it was acquired that it was subject to U.S. jurisdiction and law. Expedia voluntarily disclosed the violations, and OFAC fined Expedia $325,406.

A few important lessons can be gleaned from these enforcement actions. First, companies should practise heightened due diligence when acquiring companies that are known to have transactions in OFAC-sanctioned countries, or otherwise pose a high risk due to their geographic location. Instituting robust compliance measures, as Kollmorgen did, after acquiring a foreign subsidiary with in-person compliance training in multiple forms, reviewing customer databases, circulating memoranda informing employees of relevant U.S. sanctions and export obligations, auditing foreign subsidiaries' transactions, requiring foreign subsidiaries' senior management to certify sanctions compliance, and establishing an ethics hotline are crucial steps to mitigate any potential sanctions violations. Although Kollmorgen's compliance measures did not insulate it from complete liability, the whistleblower hotline ultimately succeeded in allowing Kollmorgen to detect the scheme implemented by Elsim's manager to circumvent sanctions.

In contrast, AppliChem and Black & Decker failed to take such extensive steps, and this likely contributed to the larger civil penalties and OFAC's determinations that their cases were egregious. Moreover, these actions demonstrate that continued monitoring, auditing, and investigating of a foreign subsidiary's operations post-acquisition are also key to mitigating sanctions risk. Foreign subsidiaries are likely to be a growing focus for OFAC enforcement actions, and companies should be prepared to perform comprehensive due diligence pre-acquisition and institute robust compliance measures post-acquisition to protect against sanctions liability.

Recent OFAC Enforcement Actions Highlight the Importance of Knowing Your Suppliers

In addition to understanding the sanctions risks that foreign subsidiaries pose, companies should also focus on supply chain due diligence, especially in locations and industries known to engage in trade with sanctioned countries or regions. Earlier this year, OFAC imposed penalties on two companies for apparent violations of sanctions laws in their sourcing practices:

- E.l.f. Cosmetics, Inc. ("ELF"): U.S.-based ELF unwittingly imported 156 shipments of false eyelashes over the course of five years from two suppliers located in China that contained materials sourced from North Korea. Throughout this period, the company's compliance programme and supplier audits focused on quality control issues rather than sanctions compliance. In imposing a fine, OFAC considered ELF's lack of a sanctions compliance programme, especially in a region that poses a high sanctions risk, to be an aggravating factor. Ultimately, ELF paid $996,080 in civil penalties to settle the action. OFAC stated that the 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 [a comprehensively sanctioned country or region] . . . is known to export goods".
- ZAG IP, LLC ("ZAG"): The U.S. company ZAG entered into a contract to supply cement clinker that it generally sourced from an Indian supplier. Before the first shipment, the Indian supplier notified ZAG that it would not have enough cement clinker to

meet ZAG's order. ZAG located an alternative supplier through a U.A.E. trading company and relied on the company's misrepresentation that the cement clinker was not subject to U.S. economic sanctions on Iran, despite knowing that the goods were produced by an Iranian manufacturer and shipped from a port in Iran. ZAG voluntarily disclosed the apparent violation to OFAC and paid a civil penalty of $506,250 to settle with OFAC.

These enforcement actions emphasise the importance of conducting comprehensive supply chain due diligence. In accordance with OFAC's emphasis on risk-based compliance, a crucial first step is to conduct a risk assessment of the company's supply chains and then to evaluate whether any products or materials actually involve input from sanctioned countries or regions. Most companies know not to source directly from sanctioned countries, but many may not realise the risk of indirectly doing so or that certain regions – as opposed to countries – are subject to sanctions. Thus, companies should begin with a risk assessment for content in their supply chain that is illicitly sourced from sanctioned countries or regions, which can include material or even labour. In guidance titled "North Korea Sanctions & Enforcement Actions Advisory",[2] OFAC has identified several "red flags" that should alert companies to a higher risk of sourcing indirectly from sanctioned countries or regions, including particular geographic areas and industries where such practices and deception are more prevalent.

The next task of determining whether a company's particular products contain content sourced from a sanctioned country or region may not be as straightforward, as some governments or businesses may try to conceal the true origin of materials or labour. Consequently, it may take a variety of different data points to confirm the source(s) of a product. For example, depending on the level of risk identified in their assessment, companies may need to enquire into: their supplier's sourcing and employment practices; complete routine onsite audits of the supplier; examine payment information related to the production of materials and bank statements; examine the supplier's ownership, product origin, and employment documentation; and investigate labelling practices. Depending on the relationship with the supplier, companies may also want to consider conducting compliance training with the foreign supplier. Companies should also incorporate sanctions compliance certifications into contract provisions with suppliers to hold suppliers accountable. Ultimately, thoroughly documenting the process taken to confirm the origin of a product will likely serve to mitigate an OFAC civil penalty.

Mitigating Enforcement Risk: Incorporating OFAC's Framework on Sanctions Compliance

In each of the enforcement actions mentioned above, OFAC provides a synopsis of where the company fell short regarding compliance. Although these *ad hoc* summaries are helpful, in a significant step to explicitly inform companies of its expectations regarding compliance, OFAC issued formal guidance titled "Framework for OFAC Compliance Commitments".[3] The Framework puts companies on notice of OFAC's expectations with respect to an effective economic sanctions compliance programme ("SCP"). OFAC makes clear that it will consider a company's SCP under the Economic Sanctions Enforcement Guidelines. An effective SCP may mitigate a civil monetary penalty for an apparent violation and will also be a factor in whether a case is deemed "egregious".

In the Framework, OFAC identifies five essential components of an SCP:

- Management Commitment: OFAC enumerates several ways senior management can show their commitment to compliance, such as having a direct reporting line between the SCP and senior management, appointing a dedicated sanctions compliance officer, allocating adequate resources to compliance units, fostering a culture of compliance throughout the organisation, and implementing remedial measures to address root causes when apparent violations occur.
- Risk Assessment: OFAC emphasises that organisations take a risk-based approach when designing an SCP and regularly conduct risk assessments. OFAC suggests an organisation conduct risk assessments of the following:
  - (i) customers, supply chain, intermediaries, and counterparties;
  - (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and
  - (iii) the geographic locations of the organisation, as well as its customers, supply chain, intermediaries, and counterparties.
- Internal Controls: OFAC recommends that an effective compliance programme have internal controls that "identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC".[4] OFAC states that SCPs should also be adaptable to the rapid changes in trade sanctions, including changes to SDN lists, updates to sanctions programmes, new executive orders, and issuance of general licences.
- Testing and Auditing: OFAC recommends routine audits of the SCP to identify programme weaknesses and deficiencies.
- Training: OFAC advises that training be provided to all relevant employees and personnel annually, at a minimum. The training should "(i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments".[5]

Since OFAC has now put companies on notice of what it expects from a SCP by this Framework, failing to take the appropriate steps identified by OFAC will likely result in increased civil penalties where sanctions violations have occurred.

DOJ and BIS Are Using Laws to Aggressively Curb Chinese Acquisition of Key Technologies

The DOJ and BIS are also carrying out the Trump Administration's ongoing trade war against China with high-profile sanctions and export controls enforcement. The Trump Administration has expressed concern about China's acquisition of key U.S. technologies and intellectual property, especially through evasion of U.S. export control laws, and diversion of the same to prohibited users such as the Chinese military.[6] In addition, China's trade relationship with North Korea is also a driver of U.S. interest in China. In apparent support of the Administration's cause, the DOJ has pressed criminal charges against key China-based businesses for trade violations, while BIS has to date designated over 130 Chinese businesses and affiliates on the Entity List in 2019.

At the centre of the trade war is China-based telecom giant Huawei Technologies Co. Ltd. ("Huawei") and its affiliates. As we discuss further below, DOJ criminally charged Huawei and its affiliates in two separate indictments, one for diverting U.S. technology to Iran and the other for stealing T-Mobile's trade secrets. Shortly thereafter, citing the DOJ indictments and asserting that Huawei "has been involved in activities determined to be contrary to national security or foreign policy", BIS added Huawei and 68 of its non-U.S. affiliates to the Entity List, which would effectively cut them off from U.S. origin technology. Several months later, BIS added another 46 non-U.S. affiliates of Huawei to the Entity List. Most recently, according to news reports, Huawei may have helped North Korea build and maintain its wireless network.[7] These reports raise concerns about whether U.S. technology was used in this project and if U.S. export controls laws were violated.

Besides the Huawei-related entities, in 2019 to date BIS has added another 15 China-based entities to the Entity List for being "involved in activities determined to be contrary to national security or foreign policy".[8] Primarily technology- and science-related, these designations include Chinese supercomputer developers and major power companies that utilise nuclear energy.

Recent DOJ and BIS Enforcement Concentrated on Huawei and Its Affiliates

The DOJ's indictments of Huawei and its affiliates demonstrate the extent to which Huawei is a threat to both U.S. national security and intellectual property. One indictment details Huawei's alleged scheme to deceive financial institutions and the U.S. government regarding Huawei's activities in Iran. In particular, the DOJ alleged that Huawei, through its employees and CFO, repeatedly misrepresented that the Iran-based business Skycom was not an affiliate of Huawei, when in fact, Huawei operated Skycom as an "unofficial" affiliate in Iran in order to dodge U.S. sanctions restrictions. The second indictment describes an alleged company-wide effort by Huawei USA to steal trade secrets from T-Mobile USA. According to the DOJ, Huawei USA was interested in stealing information on "Tappy", T-Mobile's innovative and prized robot that tests phones. As a part of the scheme, Huawei USA employees allegedly violated confidentiality and nondisclosure agreements by secretly taking photos of Tappy and even stole a piece of the robot, so Huawei engineers could replicate it.

Citing the Iran-related indictment of Huawei as raising national security and foreign policy concerns,[9] effective May 16, 2019, BIS added Huawei and 68 of its non-U.S. affiliates to the Entity List. Huawei's addition to the Entity List prohibited the export, re-export, or in-country transfer of items subject to the Export Administration Regulations ("EAR"). This means that licences are required for all exports and re-exports to Huawei of U.S.-origin goods. This broad prohibition also includes the sales of U.S. goods, sales of foreign-made items of more than a *de minimis* level of controlled U.S. content (generally 25 per cent), and even the release of controlled U.S. technology to Huawei or its listed affiliates. The prohibitions apply to persons around the world, so long as the items in question are subject to the EAR, and therefore subject to U.S. jurisdiction. Huawei and its affiliates' addition to the Entity List effectively denies them access to the U.S. supply chain, as licence applications for exports to them are subject to a presumption of denial. BIS has, however, issued a Temporary General License for certain transactions with Huawei, which it extended into November 2019, and the U.S. government has expressed that it may potentially consider granting licences for certain exports to Huawei in the future.

On May 15, 2019, just before Huawei's inclusion on the Entity List, President Trump issued a new Executive Order "Securing the Information and Communication's Technology and Services Supply Chain" ("Telecom E.O.").[10] Although the Telecom E.O. does not mention China or Huawei specifically, it is expected that the Department of Commerce will use this E.O. to further prohibit dealings with Huawei. The order authorises the Commerce Secretary to regulate from where and from whom businesses operating in the United States may acquire information and communications technology and services.[11] The Telecom E.O. does not have an immediate impact, but the Department of Commerce will implement regulations to enforce the E.O. in October 2019.

Further demonstrating Huawei's prominent role in the U.S. trade war, during the G20 summit President Trump stated his desire to relax restrictions on Huawei. However, despite these statements, at present Huawei continues to remain on the Entity List and is subject to broad export licensing requirements with a presumption of denial. It is evident that the tug-of-war with Huawei will not be resolved any time soon, and consequently businesses should remain vigilant to comply with the ever-changing U.S. sanctions and export controls relating to Huawei and its affiliates.

Other Recent BIS Enforcement Related to China

Altogether BIS added another 15 China-based entities to the Entity List in 2019 to date, targeting Chinese technology and science sectors. By their names, these entities are involved in these sectors, and were designated due to their involvement "in activities determined to be contrary to national security or foreign policy".[12] According to BIS, several have attempted to acquire U.S.-origin commodities that would ultimately provide material support to Iran's weapons of mass destruction and military programmes, in violation of U.S. export controls. Other designations included several Chinese supercomputer developers, because BIS appears to be concerned that they might support Chinese military or other government end users. Several major power companies that utilise and develop nuclear energy have also been designated because BIS states they have engaged in or enabled efforts to acquire advanced U.S. nuclear technology and material for diversion to military uses in China.

Continued Enforcement Concentrated on China

As the underlying foreign policy and national security concerns – especially diversion of U.S. technology to the Chinese military or other sanctioned end users – show no signs of abating, DOJ and BIS enforcement focused on China-based entities will likely advance along with the trade war past 2019.

Conclusion

We expect sanctions and export controls enforcement to continue to grow beyond 2019 with increasing coordination between different government agencies. As government agencies increase coordination, companies may face larger fines as each agency will likely impose its own fine. Companies would be wise to integrate OFAC's Compliance Framework into their compliance functions, dedicate enough resources to sanctions and export control compliance, and ensure that corporate affiliates abroad understand sanctions and export controls obligations. Having a robust compliance programme will help prevent enforcement actions and mitigate civil penalties.

Endnotes

1. *Treasury and Commerce Implement Changes to Cuba Sanctions Rules*, U.S. Dep't of the Treasury (June 4, 2019), https://home.treasury.gov/news/press-releases/sm700.
2. *North Korea Sanctions & Enforcement Actions Advisory*, U.S. Dep't of the Treasury (July 23, 2018), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf.
3. *A Framework for OFAC Compliance Commitments*, U.S. Dep't of the Treasury, https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf (last visited Aug. 29, 2019).
4. *Id.*
5. *Id.*
6. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, White House (June 2018), https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.
7. *Huawei secretly helped North Korea build, maintain wireless network: Washington Post*, Reuters (July 22, 2019, 8:57 AM), https://www.reuters.com/article/us-huawei-tech-northkorea/huawei-secretly-helped-north-korea-build-maintain-wireless-network-washington-post-idUSKCN1UH1GO.
8. Department of Commerce Addition of Entities to the Entity List, 84 Fed. Reg. 22,371 (June 24, 2019).

9. Department of Commerce Addition of Entities to the Entity List, 84 Fed. Reg. 22,961 (May 21, 2019).
10. Donald J. Trump, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, WHITE HOUSE (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.
11. *Id.*
12. Department of Commerce Addition of Entities to the Entity List, 84 Fed. Reg. 22,371 (June 24, 2019).

Timothy P. O'Toole is the leader of our White Collar Defense Practice Group. Between his time at Miller & Chevalier and his time in government service, Mr. O'Toole has been conducting and leading large-scale defence investigations for over 20 years. Although Mr. O'Toole has substantial experience in all areas of white collar practice, his main focus is on defending enforcement actions and conducting investigations involving the economic sanctions, export controls, and anti-money laundering laws. His clients run the gamut, including U.S. and non-U.S. financial institutions and public companies in the aviation, insurance, logistics, manufacturing, and oil and gas sectors.
Mr. O'Toole writes and speaks often about white collar defence and international trade issues at venues and media outlets around the world. He is co-chair of the National Association of Criminal Defense Lawyers (NACDL) West Coast White Collar Crime Conference in Santa Monica and a past co-chair of the NACDL's White Collar Crime Committee.

Miller & Chevalier
900 16th Street NW
Washington, D.C. 20006
USA

Tel: +1 202 626 5552
Email: totoole@milchev.com
URL: www.millerchevalier.com

Aiysha Hussain focuses her practice on internal investigations, enforcement issues, and compliance related to white collar matters, economic sanctions, export controls, and anti-bribery. Ms. Hussain counsels and represents clients on a variety of issues related to the sanctions regulations administered by the Treasury Department's Office of Foreign Assets Control (OFAC), the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), the Foreign Corrupt Practices Act (FCPA), and the False Claims Act (FCA).
Ms. Hussain is an editor of the firm's newsletter, *Focus on Iran*, a biannual publication that reports on risk and other legal issues related to developments in U.S. policy as to Iran. In 2017–2019, she was recognised as a Rising Star by *Washington, DC Super Lawyers*.

Miller & Chevalier
900 16th Street NW
Washington, D.C. 20006
USA

Tel: +1 202 626 1497
Email: ahussain@milchev.com
URL: www.millerchevalier.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group