Bloomberg Law®

bloombergbna.com

INSIGHTS: Economic Sanctions and Export Controls Update Q3 2018




By Mario Mancuso, Sanjay Mullick, Anthony Rapa and Abigail Cotterill

The View from Washington—Legislative and Regulatory Developments

Russia

The *Defending American Security from Kremlin Aggression Act of 2018* was introduced in the Senate in August 2018. If enacted, it would build on the existing *Countering America's Adversaries Through Sanctions Act* and impose additional sanctions, including those targeted at specified Russian political figures and oligarchs, in relation to the Russian energy sector, and to certain cyber actors engaging in cyber activities.

Also, the State Department's imposition of sanctions on Russia under the *Chemical and Biological Weapons Control and Warfare Elimination Act of 1991* could lead to further sanctions as of November. Notably, on November 6, the State Department announced that Russia had not provided adequate assurances regarding its chemical and biological weapons programs in accordance with the CBW Act, clearing the way for a second round of sanctions under the statute. Possible sanctions include significant trade and financial restrictions directed at Russia.

Congress' legislative activity on the Russia sanctions front, combined with OFAC's continued use of designation power to target Russian oligarchs and operatives and the State Department's use of CBW Act sanctions, suggest that U.S. sanctions on Russia have the potential to become an increased enforcement priority in 2019.

North Korea

In July 2018, OFAC, in coordination with the U.S. Department of State, the U.S. Department of Homeland Security Customs and Border Protection (''CBP''), and Immigration and Customs Enforcement (''ICE''), issued a ''North Korea Sanctions & Enforcement Actions Advisory'' (''*the Advisory*'') which warned of the risk associated with inadvertent sourcing of North Korean goods, services, or technology, or of the presence of North Korean nationals in the supply chain (U.S. Department of State, Jul. 23, 2018). The Advisory emphasizes that companies should guard against the inadvertent presence of North Korean goods, services, technology, or labor in the supply chain through the implementation of effective due diligence policies, procedures, and internal controls. It underscores that knowingly conducting or facilitating trade with North Korea, or facilitation of a significant transaction on behalf of a person designated under a North Korea-related Executive Order, could lead OFAC to impose sanctions on persons including those who have engaged in at least one ''significant'' import or export of goods, services, or technology from North Korea.

Enforcement Developments There were a limited number of enforcement announcements in this quarter. We assess the relative paucity of enforcement matters to be arbitrary and unrelated to any larger shift in enforcement priorities. Indeed, we believe the surge in recent regulatory developments (and related Congressional interest) portend a future uptick in enforcement in the medium term.

Cyber Attacks

On September 6, 2018, OFAC designated North Korean citizen Park Jin Hyok and North Korean

government-backed company Chosun Expo Joint Venture (''KEJV'') on the Specially Designated Nationals and Blocked Persons List (''SDN List''), freezing their assets in the United States and prohibiting U.S. persons from dealing with them. Treasury Secretary Mnuchin announced the sanctions were part of the U.S. policy to ''hold North Korea accountable'' for irresponsible ''state behavior in cyberspace'' (U.S. Department of the Treasury, Sept. 6, 2018). That same day, the U.S. Department of Justice (''DOJ'') announced criminal charges against Park for conspiring to conduct significant cyberattacks from 2014 to 2017, including the ''WannaCry 2.0'' ransomware attack (U.S. Department of Justice, Office of Public Affairs, Sept. 6, 2018). According to the complaint, Park worked for KEJV and a similar entity called Lazarus Group to conduct a series of cyberattacks on the ''entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities.'' *Id.* The actions targeting Park and KEJV demonstrate that the U.S. Government will use every tool at its disposal, including asset freezing, travel bans, and criminal prosecution, to combat malicious cyber activity. Notably, entities affiliated with foreign governments, and those acting at their behest, are not beyond the reach of enforcement authorities. In fact, Executive Order 13722, the authority under which OFAC blocked Park and KEJV, specifically provides for the blocking of the Government of North Korea and persons that engage in malicious cyber activity on its behalf.

Distributors

On September 14, 2018, Epsilon Electronics Inc. (''Epsilon'') agreed to settle for $1.5 million charges it violated the *Iranian Transactions Sanctions Regulations* (''ITSR'') (U.S. Department of the Treasury, Office of Foreign Assets Control, Sept. 13, 2018). OFAC had found that Epsilon violated the ITSR by selling to a distributor in the UAE with knowledge that the distributor frequently sold into Iran. Epsilon had challenged an initial $4.07 million penalty issued by OFAC in July 2014 for the same activities. The D.C. Circuit Court remanded the case to OFAC in May 2017 after finding that OFAC's investigation for some of the alleged transactions was insufficient. The case was notable in upholding OFAC's interpretation of the transshipment restriction set out at 31 C.F.R. § 560.204. The September 2018 penalty took into account Epsilon's cooperation with OFAC and implementation of remedial measures, including terminating the relationship with the distributor. The case illustrates that the U.S. Government continues to bring enforcement actions related to the illegal provision of goods and services by the technology, aviation, and financial industries to Iran, especially through third countries outside of the United States.

Financial Institutions

After settling charges in June 2018 related to bribery in Libya with both the U.S. Department of Justice and the French Parquet National Financier, the French bank Société Générale (''SocGen'') announced in September 2018 that it anticipates penalties for U.S. sanctions violations of approximately $1.4 billion (*Bloomberg*, Fabio Benedetti-Valentini and Geoffrey Smith, Sept. 3, 2018). SocGen is in ongoing discussions with OFAC regarding allegations that it violated U.S. sanctions, but public reports do not indicate whether those violations relate to Libya or to additional countries or persons subject to U.S. sanctions. If the final penalty amount is close to the $1.4 billion expectation, the case will be one of the highest penalties imposed by OFAC to date.

Termination of ZTE Denial Order

On July 13, 2018, BIS terminated an April 15, 2018, order that had denied all export privileges of Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd. (collectively ''ZTE''), prohibiting U.S. companies from supplying to ZTE items subject to the *Export Administration Regulations* (''EAR''). BIS terminated the denial order after ZTE paid $400 million into an escrow account in settlement of allegations that ZTE had misled BIS during discussions leading up to a March 2017 settlement. That settlement related to allegations that ZTE had violated the EAR by re-exporting certain export-controlled equipment to Iran. The $400 million escrow payment was in addition to $1 billion in penalties that ZTE paid to BIS earlier this year, which in turn were on top of $892 million in penalties that ZTE had paid as part of the prior settlement.

BIS's termination of the denial order followed a June 8, 2018, Superseding Order which approved a settlement between BIS and ZTE; provided for payment of the penalties described above; required that ZTE replace its Board; and imposed extensive compliance obligations on ZTE. These included that it retain at its expense a ''Special Compliance Monitor'' to oversee its compliance with U.S. export controls and sanctions laws that was both selected by and answerable to BIS itself. The requirements of the monitorship include significant auditing and extensive training for leadership, management, and employees of both the company and its worldwide affiliates over which it exercises ownership and control, as well as that ZTE publish on its website the export control classification of all items subject to the EAR that it deals in. The settlement demonstrates the significant leverage that denial orders provide the U.S. Government over companies whose supply chains are reliant on U.S. technologies.

Chinese Front Companies

On August 22, 2018, DOJ announced the sentencing of a Canadian national to over three years in prison for conspiracy to unlawfully export U.S. goods to Iran (U.S. Department of Justice, Aug. 22, 2018). The Canadian national had created several front companies in China to filter U.S.-origin export-restricted technology products to agents of the Iranian Department of Defense. The various goods exported included sensitive missile and advanced manufacturing components as well as certain thermal imaging cameras. Several shipments included falsified shipping documents that were searched and seized by U.S. law enforcement agencies prior to export. The investigation into this transshipment and the sentence imposed indicates investigators' interest in disrupting front companies that may be used by foreign nationals to violate export controls. Like the ZTE settlement, this enforcement action demonstrates export control regulators' focus on disrupting channels of diversion of U.S. products from China to Iran and other restricted jurisdictions. Continued coordination by OFAC and BIS with U.S. Government agencies including DOJ and State underscores that in addition to des-

ignations on prohibited parties lists, there is the potential for criminal penalties in cases where the U.S. Government finds knowing violations of U.S. economic sanctions and export controls laws.

Trade Diversion to Iran and Crimea

On September 4, 2018, BIS designated two Turkish entities on the Entity List for attempting to obscure the U.S. origin of certain aircraft engines and other parts as part of a scheme to supply these parts to users in Iran (U.S. Department of Commerce, Bureau of Industry and Security, Sept. 4, 2018). The September 2018 designations also included certain Russian entities that are affiliated with PJSC Mikron, an entity designated for its activities related to the Crimea region of Ukraine. Such designations show that BIS remains focused on enforcing the sanctions and export control restrictions regarding the Crimea region of Ukraine and potential risks associated with doing business with Russian entities (or affiliates thereof) with operations or activities relating to Crimea.

Key Compliance Takeaways

■ Third party distributors and agents continue to pose compliance and enforcement risks, and necessitate risk-tailored due diligence and monitoring to mitigate such risks for the duration of the third-party relationship

■ Strong end user checks designed to identify front companies posing as *bona fide* end users or customers are critical to mitigating export controls risks.

■ Confidential ethics hotlines can promote a culture of compliance and create opportunities to remediate and secure voluntary disclosure credit related to isolated ''bad actors'' before would-be whistleblowers report outside of the Company.

Mario Mancuso leads the International Trade and National Security practice at Kirkland & Ellis LLP, providing strategic and legal advice to companies, private equity sponsors, and financial institutions operating or investing across international borders.

Sanjay Mullick, a partner at Kirkland & Ellis LLP, advises companies, sponsors and investors on export controls and sanctions risk assessment in conjunction with investments, offerings and mergers and acquisitions.

Anthony Rapa, a partner at Kirkland & Ellis LLP, counsels companies, financial institutions, and private equity sponsors worldwide regarding regulatory compliance in the context of cross-border operations and investments.

Abigail Cotterill, Of Counsel at Kirkland & Ellis LLP, provides legal advice to companies, financial institutions, and private equity sponsors on the regulatory and other risks of operating or investing across international borders.