Bloomberg Law

International Trade Daily Bulletin™

EXPORT CONTROLS

Recent Developments and Trends in Economic Sanctions and Export Controls Enforcement and Expected Changes Ahead

By Jeremy Zucker, Darshak Dholakia, Hrishikesh Hari, and Jacob Grubman

I. Introduction

If presidential campaign rhetoric is any indication of future policy, the compliance community should prepare for change. The transition from President Barack Obama to President Donald Trump is expected to result in potentially significant modifications of sanctions against Cuba, Iran and/or Russia, as well as export controls applicable to a range of industries.

Across administrations, economic sanctions and export controls have been viewed as indispensable weapons in the U.S. foreign policy arsenal. As U.S. Treasury Secretary Jacob J. Lew stated in remarks at the Carnegie Endowment for International Peace in March 2016: ''Economic sanctions have become a powerful force in service of clear and coordinated foreign policy objectives—smart power for situations where diplomacy alone is insufficient but military force is not the right response. They must remain a powerful option for decades to come.''

This article describes the U.S. government's current export and sanctions-related priorities, highlights recent enforcement actions that effectuate these priorities, and discusses recent changes in export laws and regulations. This article also identifies changes that might come to pass under the administration of President Trump. In the midst of this shifting landscape, companies will need to continue to assess their exposure to changes in these laws and regulations.

Jeremy Zucker is a partner and Darshak Dholakia, Hrishikesh Hari, and Jacob Grubman are associates in the International Trade and Government Regulation practice in the Washington, D.C., office of Dechert LLP.

II. Export Controls Enforcement and Economic Sanctions Enforcement Trends

Under the Obama administration, the U.S. government focused export controls and economic sanctions enforcement in six key areas:

1. Preventing the use of U.S. technologies and information on weapons of mass destruction;
2. Reducing the acquisition of advanced U.S. military technology by potentially adverse militaries;
3. Stopping the pilfering of U.S. technologies and information for terrorist activities;
4. Encouraging voluntary disclosure of corporate misconduct;
5. Deterring diversion of controlled U.S. technology and information to rogue actors and adverse militaries; and
6. Combatting cyber intrusions in the U.S. and/or involving U.S. businesses.

Each agency charged with enforcing U.S. export controls and sanctions has brought actions to effectuate these priorities in recent years. The Treasury Department's Office of Foreign Assets Control (''OFAC'') enforces U.S. sanctions requirements, and the Commerce Department's Bureau of Industry and Security (''BIS'') enforces U.S. dual-use export controls. Meanwhile, the State Department's Directorate of Defense Trade Controls (''DDTC'') handles defense trade matters, and the Justice Department's National Security Division (''NSD'') wields criminal enforcement jurisdiction.

a. U.S. Economic Sanctions Enforcement. OFAC is responsible for administering U.S. economic sanctions programs (*see Civil Penalties and Enforcement Infor-*

 ISSN 0000-0000

mation, U.S. Department of the Treasury). During Fiscal Year 2016, OFAC resolved just under 1,000 investigations, with less than 2 percent resulting in public enforcement action (with 12 settlements and six Findings of Violations). In addition, OFAC designated 1,005 individuals and entities on the List of Specially Designated Nationals and Blocked Persons and other U.S. sanctions lists during FY 2016, and delisted 957 individuals and entities over that period.

While OFAC has engaged in more investigations and taken more action in designating and delisting entities than in the past, its settlement figures were down in (calendar year) 2016. OFAC concluded the calendar year with its lowest settlement total since 2008, around $21.6 million for the year, reflecting a break in the office's run of enforcement actions against global banks, as discussed below. OFAC's nine civil settlements with companies in other industries also marked the fewest since 2006.

Since 2009, OFAC has entered into 10 civil settlements with financial institutions, each involving penalties in excess of $100 million. Those 10 settlements resulted in over $3.75 billion in penalties, accounting for 90 percent of OFAC's settlement total over that period. The string of enforcement actions against global banks reached its pinnacle in 2014, when OFAC settled with BNP Paribas for over $963 million—accounting for nearly a quarter of OFAC's settlement amount from 2009 to 2016. In connection with its settlement with the U.S. government, BNPP was ordered to forfeit $8.83 billion and to pay a fine of $140 million. In separate settlements, BNPP agreed to pay $508 million to the Board of Governors of the Federal Reserve System and $2.24 billion to the New York State Department of Financial Services—payments for which BNPP earned credit against its payment to the U.S. Department of Justice (''DOJ'')—and $963 million to OFAC, which was satisfied by BNPP's payment to the DOJ.

OFAC's most recent significant enforcement action against a financial institution was in October 2015, when it reached a settlement with Crédit Agricole Corporate and Investment Bank (''Crédit Agricole'') for nearly $330 million. (In January 2017, Toronto-Dominion Bank, a Canadian institution, entered into a settlement agreement with OFAC under which it paid approximately $500,000 in connection with violations of U.S. sanctions against Iran and Cuba.) The Crédit Agricole settlement illustrates OFAC's approach to enforcement, focusing on thousands of transactions that Crédit Agricole and its predecessor banks and subsidiaries processed on behalf of entities and individuals in sanctioned countries (including Burma, Cuba, Iran and Sudan) in contravention of several U.S. sanctions policies. As reflected in the settlement materials, OFAC found that in processing these transactions Crédit Agricole officials acted with knowledge of the violations and implemented reporting practices designed to prevent detection of the violations by U.S. financial institutions. In each other instance of enforcement against a global financial institution, OFAC found either similar measures designed to elude detection by enforcement authorities or willful and reckless conduct by bank officials.

The Crédit Agricole case also included many of the aggravating factors cited by OFAC in the settlements with other financial institutions. Among those factors were Crédit Agricole's early knowledge of potential violations, the company's sophistication and global presence, the company's lack of appropriate controls, and the substantial harm its conduct caused to the objectives of OFAC's sanctions programs. Full voluntary disclosure has been the exception in these enforcement actions, with the only instances being Barclays in 2010 and Standard Chartered in 2012. At the same time, once involved in enforcement proceedings, most banks have cooperated with OFAC and have received settlement credit for their cooperation; only ING (2012) did not. Crédit Agricole's fine was mitigated because of its cooperation, its history of compliance, and its remedial response.

The pattern of enforcement actions against major banks reflects OFAC's desire to restrict access of sanctioned parties to the U.S. financial system.

b. U.S. Export Controls Enforcement. BIS enforces U.S. export controls laws and administers the Export Administration Regulations (''EAR''). During FY 2016, BIS brought 39 administrative actions against businesses and individuals, resulting in over $23 million in civil penalties. BIS investigations also resulted in the criminal conviction of 32 individuals and businesses, with over $79 million in forfeitures and around $275,000 in criminal fines.

Arguably BIS's most significant civil enforcement action in recent years came in March 2016, when it added Chinese telecom titan Zhongxing Telecommunications Equipment Corporation (''ZTE'') and three of its subsidiaries to the Entity List for using shell companies to evade U.S. export controls and economic sanctions measures (Additions to the Entity List, 81 Fed. Reg. 12004 (Mar. 8, 2016)). ZTE and its subsidiaries allegedly imported U.S.-origin goods and reexported them to Iran and other prohibited destinations pursuant to a plan specifically adopted to circumvent U.S. export controls, according to an internal document labeled ''Top Secret *Highly Confidential*'' that was specifically authorized by senior management—and which, notably and unusually, was published by BIS.

After a four-year investigation, BIS added ZTE and the subsidiaries involved in the scheme to the Entity List, imposing on them a license requirement for the export, reexport, or transfer of any item subject to the EAR. In addition, BIS indicated that it would deny ZTE's license applications, effectively barring the company from accessing U.S. components and inputs. In the weeks following the enforcement action, however, BIS issued a temporary license to ZTE in exchange for undisclosed concessions. Since then, BIS has added further ZTE subsidiaries to the Entity List but has extended ZTE's temporary license repeatedly, with the license currently set to expire in February 2017. While BIS has allowed ZTE to continue to transact in U.S. origin goods, its penalties against ZTE align with the U.S. government's stated interest in preventing transactions with entities connected to proliferation and terrorism.

c. Defense Trade Controls Enforcement. DDTC regulates international defense trade through the International Traffic in Arms Regulations (''ITAR'') and the Arms Export Control Act (''AECA''). Over the past decade, DDTC has entered into 22 penalty and oversight agreements totaling nearly $322 million in civil fines, in addition to other undertakings. The agency's two most recent penalty and oversight agreements demonstrate its strict enforcement of defense trade restrictions.

  ITD ISSN 0000-0000

DDTC settled with Marc Turi and Turi Defense Group, Inc. (together, ''Turi'') for violations of the ITAR and the AECA in October 2016. Turi, a broker of defense articles, facilitated the transfer of defense articles between foreign nations, sometimes in furtherance of U.S. government contracts and interests. According to settlement materials, in 2011, Turi requested authorization to broker the transfer of defense articles to Libya but was denied. Turi did, however, receive authorization to broker a transaction on behalf of the Government of Qatar involving $267 million in Eastern European armament and ammunition. Turi subsequently attempted to divert the approved transaction to Libya and drafted a proposal to the Libyan interim prime minister that included a nearly identical list of arms included in the approved transaction. Both actions constituted violations, as the ITAR prohibit both proposing and facilitating the transfer of defense articles to Libya without DDTC authorization. For the violations, Turi agreed to pay a $200,000 civil penalty and, more significantly, to refrain from participating in activities subject to the ITAR for four years, effectively barring Turi from operating in the defense industry during that period. ITAR restrictions can apply regardless of whether a company is operating internationally or domestically, and the ITAR apply to all products on the U.S. Munitions List as well as related technical data and defense services. Violations such as this, then, can have significant and lasting consequences on companies operating in this industry. The foregoing restrictions reflect the DDTC's interest in blocking the transfer of U.S. defense articles to entities connected to WMD proliferation and terrorism. While the company did not disclose voluntarily, the company received partial mitigation credit for cooperating with DDTC's investigation and because its violations did not result in the actual transfer of any defense articles.

d. Criminal Enforcement. The Justice Department's National Security Division (''NSD'') targets terrorism and other threats to national security. In this context, the NSD investigates and prosecutes export violations involving national security, foreign relations and the export of military and strategic products and technologies. In 2015, NSD brought charges in approximately 60 export and sanction cases. While nearly half concerned Iran according to remarks in May 2016 by the Chief of NSD's Counterintelligence and Export Control Section, we highlight below enforcement matters involving unauthorized exports to China and Russia.

In March 2016, Su Bin, a Chinese national and resident, pleaded guilty to conspiring to hack into U.S. defense contractors' computer networks and send sensitive military and export-controlled data to China. From 2008 to 2014, Su and two coconspirators, who were Chinese military officers, executed a scheme to access computer networks in the U.S. to purloin technical data listed on the U.S. Munitions List. Su and his coconspirators would communicate via email, with the latter providing Su with file information from the targeted networks. On Su's instructions, the coconspirators hacked specific files and transferred the data to Su, who translated it from English into Chinese and sent it on to a recipient in China. In February 2016, Su waived extradition and consented to be transported to the U.S. for trial. Five months later, he was sentenced to 46 months in federal prison.

In September 2015, Alexander Fishenko, a dual citizen of the U.S. and Russia, pleaded guilty to acting as an agent of the Russian government and conspiring to illegally export microelectronics to Russia, in addition to wire fraud and money laundering. An owner and executive of a Houston-based export company and a Moscow-based procurement company, Fishenko worked with a network of fellow defendants to send high-tech microelectronics—including analog-to-digital converters, static random access memory chips, microcontrollers, and microprocessors—to Russian military and intelligence agencies. Over the course of their conspiracy, Fishenko and the others evaded U.S. export controls, and the Russian Ministry of Defense certified Fishenko's company to procure and deliver military electronics. For his role, Fishenko was sentenced to 10 years in prison in July 2016. The prosecution was noteworthy for the involvement of microelectronics commonly used in military systems, which Russia does not produce in significant numbers.

Both the Su and Fishenko prosecutions highlight the NSD's emphasis on keeping U.S. defense technology out of the hands of adverse militaries and protecting U.S. companies from cyberattacks.

III. Developments to Monitor

In addition to enforcement actions effectuating stated priorities, several agencies have issued rules and statements indicating changes to enforcement practices and policies. Export control and sanctions enforcement will evolve in conjunction with these recent and forthcoming policy changes.

a. NSD Voluntary Self-Disclosure Guidance. The NSD released new guidance on Oct. 2, 2016, detailing its policy of encouraging businesses to voluntarily self-disclose violations of U.S. export control and sanctions rules (U.S. Dept. of Justice, *Guidance Regarding Voluntary Self-Disclosures, Cooperation, and Remediation in Export Control and Sanctions Investigations Involving Business Organizations* (October 2, 2016)). Mirroring the April 2016 Foreign Corrupt Practices Act self-disclosure pilot program introduced by the Justice Department (*see* U.S. Dept. of Justice, Criminal Division, *The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance* (April 5, 2016)), the new NSD guidance establishes the criteria for adjusting penalties in cases of voluntary self-disclosure of export control and sanctions violations.

In general, the DOJ assesses penalties in light of the Principles of Federal Prosecution of Business Organizations (''USAM Principles'') and certain fine provisions of the U.S. Code. The new NSD guidance supplements both sets of considerations by granting additional credit to companies who meet all of the program's requirements. The NSD will consider that credit when determining the type of disposition to a case, the extent of fine reductions and the need for a monitor. The policy grants credit to companies that voluntarily self-disclose violations, fully cooperate with government authorities, and work to remediate compliance programs and disgorge ill-gotten gains. The new guidance also illuminates several factors that may aggravate penalties for violations.

The NSD guidance includes strict standards for earning credit for voluntary self-disclosure. To count as voluntary, a company's disclosure must be complete and prompt and must be made prior to an imminent threat

of investigation. In this respect, the new guidance furthers the standards set forth in the so-called Yates Memorandum, in which the U.S. government emphasized that, in order to be eligible for any cooperation credit whatsoever (in both criminal and civil cases), corporations must provide the DOJ with all relevant facts about individuals involved in corporate misconduct (Memorandum from Sally Quillian Yates, Deputy Att'y Gen., U.S. Dep't of Justice, on Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015)). The new NSD guidance further emphasizes that assessment of remediation efforts will focus on a variety of factors that include the culture of compliance, the resources dedicated to the compliance program, and the timeliness of remedial measures implemented by a company.

Businesses that meet each of the standards set forth under the new guidance are eligible for benefits, including, among others, a non-prosecution agreement, a reduced period of supervision, a reduced fine, and the elimination of a monitor. The guidance also details several aggravating factors that may result in greater penalties, including exports related to nuclear proliferation, weapons of mass destruction and terrorism; repeated violations; knowing involvement of upper management; and significant profits from criminal violations.

Some concern has arisen regarding disclosure to both the DOJ and other administrative agencies. While BIS and OFAC also have released guidelines encouraging voluntary self-disclosure, some company representatives have raised the possibility that disclosure to the DOJ indicates the presence of willful conduct to other enforcement agencies. DOJ officials have emphasized the absence of a penalty for failure to voluntarily self-disclose violations and the already cooperative approach taken by the DOJ and other agencies in enforcing export control and sanctions laws.

A decision of whether and when to disclose is always fact-specific and should be considered with the advice of counsel. While there appear to be potential benefits from the new guidance, the government's decision to provide credit to companies who disclose remains discretionary and companies are therefore not guaranteed the benefits of the program. The timing of any voluntary disclosure (e.g., before, during or after an internal investigation has been conducted) also should be carefully considered. There is a risk, for example, that the DOJ might ask a company to pause its own investigation to allow the DOJ to be the first to interview potential witnesses. This could result in companies delaying disclosures to other agencies, such as OFAC and BIS, as well as delays in reports to corporate boards regarding the status of the investigation.

b. Updated BIS Voluntary Disclosure Guidance. In June 2016, BIS issued a final rule revising the agency's voluntary disclosure guidance in an apparent attempt to harmonize its enforcement practices with OFAC's enforcement practices (Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases, 81 Fed. Reg. 40499 (June 22, 2016) (to be codified at 15 C.F.R. Part 766)). BIS employs a range of disciplinary measures in response to export control violations. Where an individual willfully violates export control laws, BIS can refer the case to DOJ, which may apply maximum penalties of 20 years of imprisonment or $1 million per violation. In the absence of reckless or willful misconduct, BIS may seek civil penalties of up to $284,582 or twice the value of the transaction (whichever is greater). Alternatively, BIS may conduct an administrative enforcement proceeding resulting in fines, license revocation, or other sanctions, or it may issue no-action or warning letters.

In its revised guidelines, BIS emphasized the steps companies can take to receive mitigation of penalties for export control violations. The agency particularly highlighted the value of voluntary self-disclosure. Underscoring the history of lenience for cases involving voluntary self-disclosure, BIS instituted a rule granting a 50 percent reduction in maximum penalties for cases where violations are self-disclosed. The new guidelines further emphasize risk-based compliance programs in alignment with the agency's Export Management System Guidelines, the presence of which may serve as an additional mitigating factor. Pursuant to this, BIS explained that it would seek employee training, audits, and other undertakings related to compliance and that, in some cases, it would suspend penalties where companies apply the value of such fines to the development of compliance programs.

The new BIS guidelines add greater clarity to the agency's approach to settlements involving voluntary self-disclosure, though some uncertainty remains for companies considering disclosure. Importantly, the guidelines apply only to settlements and not to litigation (nor to the anti-boycott regulations of the EAR). In addition, BIS retains broad enforcement discretion, a level of authority that may impact cases of ''egregious'' violations, where the new 50 percent penalty reduction may not always apply. Furthermore, just as the new DOJ guidance may raise concerns about the appearance of a disclosure to the DOJ (and the implication of willful misconduct), the BIS guidelines do not specifically address the potential for the agency to refer disclosures to the DOJ, possibly resulting in greater penalties for companies. As the new guidelines neither compel voluntary self-disclosure nor provide comprehensive penalty criteria, companies should work with counsel to determine whether and how best to submit disclosures to enforcement authorities.

c. Changes to Economic Sanctions Programs and Potential Penalties. The U.S. Government has reformed its sanctions requirements for Iran, Cuba and Burma/Myanmar (among others) in recent years, while imposing new sanctions against certain Russian entities and individuals. While the reform measures authorize certain parties to engage in specified activities relating to both countries, federal officials have indicated their intent to continue active enforcement of violations of the sanctions requirement that remain. Pursuant to this objective, OFAC has increased the maximum civil penalties available for violations of each of the regulatory programs it enforces.

1. Changes to Sanctions Programs. Over the last two years, the U.S. Government has made significant modifications to some of its most prominent sanctions programs. In December 2014, Obama announced the restoration of diplomatic ties between the U.S. and Cuba, with regulatory amendments easing certain sanctions requirements over the following months. In January 2015, the U.S. joined the member states of the European Union and the United Nations in signing the Joint Comprehensive Plan of Action (''JCPOA''), which removes certain sanctions with respect to Iran. Obama

  ITD ISSN 0000-0000

followed these policy changes by removing the ''national emergency'' classifications that limited trade to Côte d'Ivoire and Burma/Myanmar in September and October 2016, respectively, which effectively terminated sanctions regulations maintained by OFAC with respect to those countries. In addition, on January 13, 2017, Obama issued an executive order in his final days in office effectively suspending all U.S. economic sanctions on Sudan (also known as the Republic of Sudan or North Sudan). Under a new general license to the Sudan Sanctions Regulations issued by OFAC, U.S. persons now are permitted to engage in a wide range of financial transactions involving Sudan that previously were prohibited, including processing transactions on behalf of persons in Sudan and dealing in previously-blocked property of the Government of Sudan (*see, e.g.*, *Sudanese Sanctions Regulations, Final Rule*, U.S. Dept. of Treasury, 82 Fed. Reg. 4793 (Jan. 17, 2017)). However, restrictions remain on exports of most items specifically controlled on the EAR's Commerce Control List.

In each instance, the U.S. government has indicated its intention to continue enforcement efforts for conduct not made legal by the recent policy changes. U.S. agencies, for example, will continue active enforcement of restrictions against transactions between U.S. persons and Iranian parties, with emphasis on the Islamic Revolutionary Guard Corps and other entities contributing to nuclear proliferation. In addition, restrictions continue to apply to transactions with persons or entities that remain on the SDN List.

The U.S. government demonstrated its willingness to pursue additional sanctions when it instituted new sanctions against certain Russian entities and individuals in December. Obama initially authorized sanctions against computer hackers pursuant to an Executive Order issued in 2015. In December 2016, Obama amended the prior order specifically to enable sanctions against parties that use cyberattacks that target U.S. elections and used the new authority to sanction eleven Russian entities and individuals (*see, e.g.*, The White House, *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment* (Dec. 29, 2016)).

2. Increases in Maximum Civil Penalties. In an interim final rule published in July, OFAC announced increases to the maximum civil penalties available for violations of several regulations under its authority (*see* Implementation of the Federal Civil Penalties Inflation Adjustment Act, 81 Fed. Reg. 43070 (July 1, 2016)). The new penalties, listed in the table below, are effective for violations that occurred after Nov. 2, 2015. OFAC generally charges companies with violations of regulations promulgated pursuant to the International Emergency Economic Powers Act. (These include the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560; the Sudanese Sanctions Regulations, 31 C.F.R. part 538; and the Weapons of Mass Destruction Proliferators Sanctions Regulations, 31 C.F.R. part 544. OFAC also commonly issues charges pursuant to Executive Order 13382 of June 28, 2005, ''Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters,'' and the Cuban Assets Control Regulations, 31 C.F.R. part 515.)

Statute	Prior Penalty Amount	Penalty Amount Effective August 1, 2016
Trading With the Enemy Act	$65,000	$83,864
International Emergency Economic Powers Act	Greater of $250,000 or twice the amount of the underlying transaction	Greater of $284,582 or twice the amount of the underlying transaction
Antiterrorism and Effective Death Penalty Act of 1996	Greater of $55,000 or twice the amount of which a financial institution was required to retain possession or control	Greater of $75,122 or twice the amount of which a financial institution was required to retain possession or control
Foreign Narcotics Kingpin Designation Act	$1,075,000	$1,414,020
Clean Diamond Trade Act	$10,000	$12,856

In addition to civil penalties, the enforcement examples discussed above demonstrate that there can also be significant reputational harm and other penalties (e.g., suspension of export privileges) resulting from violations of these laws. Companies should remain vigilant in assessing their exposure to such laws.

d. Export Control Reform Initiative. The Export Control Reform Initiative (''ECRI'') is an effort to simplify and consolidate U.S. export control rules (*see About Export Control Reform (ECR)*, Export.gov; *Export Control Reform: Control Lists ''Tracker''*, Export.gov). Specifically, the ECRI focuses on revising the U.S. Munitions List in order to streamline the export process while maintaining restrictions that enhance national security. Under the new regulations, the U.S. government has moved relatively less sensitive items from the Munitions List to the newly created 600 Series of export control classification numbers on the Commerce Control

List, which it hopes will facilitate commerce among U.S. allies and partners while retaining security controls.

Since 2009, the ECRI has resulted in revisions to 18 of the 21 categories of the Munitions List. In 2016 and so far in 2017, BIS and DDTC have issued proposed and final rules addressing a number of categories on the Munitions List, including Category VIII (Aircraft and Related Articles), Category XII (Fire Control and Lasers), XIV (Toxicological Agents), Category XV (Spacecraft and Related Articles) and Category XIX (Gas Turbine Engines). Proposals for the final three Munitions List categories not yet covered by any reform efforts (Firearms, Artillery, and Ammunition) have not yet been released.

IV. Looking Ahead

The new Trump administration has indicated its intention to revisit some of the recent modifications to U.S. sanctions programs. During and after his presidential campaign, Trump was critical of the Obama administration's negotiations on several trade fronts. Addressing the rapprochement between the U.S. and Cuba, Trump tweeted in November, ''[i]f Cuba is unwilling to make a better deal for the Cuban people, the Cuban/American people and the U.S. as a whole, I will terminate the deal''. Trump was also harshly critical of the Iran agreement, describing it during a presidential debate as ''the stupidest deal of all time'' (*see, e.g.*, Najmeh Bozorgmehr, *Iran measures response to Donald trump's election victory*, Financial Times (Nov. 17, 2016)).

The new administration and Congress appear to share a desire to renegotiate or withdraw from the JCPOA. In October, Vice President Mike Pence said that Trump would ''rip up the Iran deal'' (though advisers have since tried to soften that stance) (*see, e.g.*, Jose A. DelReal, *Trump and advisers back off major campaign pledges, including Obamacare and the wall*, Chicago Tribune (Nov. 12, 2016)). Meanwhile, Congress voted in November to extend the President's authority to impose sanctions against Iran for another decade, meaning that the U.S. has preserved its ability to ''snap back'' sanctions against Iran in the event of a departure from the accord. Because the agreement is non-binding on the U.S. and the President wields significant authority with respect to the Iran sanctions program, the new administration will have broad discretion in determining its direction. The first major test of the new administration's stance on Iran came to the fore in December, when Boeing Co. reached a deal to sell 80 jetliners to Iran. The deal drew criticism from certain Republican lawmakers, and its financing is likely contingent on approval from Treasury and State Department officials, as well as Congress (*see, e.g.*, Robert Wall & Asa Fitch, *Boeing Seals Nearly $17 Billion Iran Deal*, Wall Street Journal (Dec. 11, 2016)). Regardless of any unilateral steps the new administration takes with respect to reimposing sanctions on Iran, a future sanctions program would be constrained by multilateral participation from, among others, the United Nations and European Union.

The Obama administration's renewal of diplomatic and economic relations with Cuba may also be at risk under the new administration. While the U.S. embargo remains largely in place, Obama has eased sanctions against Cuba in recent years through executive action, the same authority that would allow Trump to reimpose restrictions. Trump's hiring of pro-embargo transition team members may be viewed as one indication that he will move to reinstate certain sanctions on Cuba, which might include returning Cuba to the list of state sponsors of terrorism and reinstituting travel and business constraints (*see, e.g.*, Julie Hirschfeld Davis, *Fate of U.S.-Cuba Thaw Is Less Certain Under Donald Trump*, New York Times (Nov. 26, 2016)). In addition, Congress has given little indication that it will repeal the statutory embargo that remains in place.

The Trump administration likely faces greater political obstacles in its pursuit of a refreshed relationship with Russia, which may include easing certain sanctions imposed as a result of the geopolitical crisis in Ukraine. In the aftermath of allegations that the Russian government used computer hacking to influence the Presidential election—allegations subsequently supported by a declassified report released by the Office of the Director of National Intelligence in January—several members of Congress indicated their support for continuing sanctions against Russia. Trump, however, has continued to signal his intention to bring about improved relations with Russia, commenting in a January press conference, ''[I]f Putin likes Donald Trump, I consider that an asset, not a liability'' (*see*, New York Times, *Donald Trump's News Conference: Full Transcript and Video* (Jan. 11, 2017)). During his Senate confirmation hearing, Secretary of State nominee Rex Tillerson stated that he would have pursued a stronger response to Russia's annexation of Crimea in 2014, but he also refrained from clearly expressing his opinions of the existing sanctions regime. Easing sanctions against Russia in this political climate may be difficult for the new administration. However, as is the case with respect to the Cuba sanctions, the new administration will have at least discretion with respect to the future of Russia sanctions.

As of the date of this article, Trump had not yet commented on the easing of sanctions against Sudan in Obama's final days in office. As the easing was accomplished by executive order, Trump has the authority to unilaterally reimpose sanctions. However, public reports indicate that the Trump administration was fully aware and supportive of the move.

V. Conclusion

The enforcement priorities and trends described herein reflect the decisions of the Obama administration. While these priorities will inform ongoing enforcement actions into the start of the new administration, export controls and sanctions policies may change under Trump. Given this and the constantly shifting geopolitical landscape, companies should continue to monitor the ways in which economic sanctions and export controls impact their business.

  ITD ISSN 0000-0000