

Drinker Biddle

Update on U.S. Export Controls and Sanctions Enforcement

Nate Bolin & Pete Baldwin

June 26, 2019

Agenda

1. Overview
2. Export Control and Sanctions Law Changes
3. Enforcement Update

1. Overview

Key Agencies and Regulations

- U.S. Department of the Treasury, Office of Foreign Assets Control (**OFAC**)
 - Sanctions programs
 - Embargoed destinations/parties
- U.S. Department of State, Directorate of Defense Trade Controls (**DDTC**)
 - International Traffic in Arms Regulations (ITAR)
 - Defense/military items and services on the U.S. Munitions List (USML)
- U.S. Department of Commerce, Bureau of Industry and Security (**BIS**)
 - Export Administration Regulations (EAR)
 - Commercial/dual-use items on the Commerce Control List (CCL)
 - Census Bureau – Foreign Trade Regulations (FTR)
- U.S. Customs and Border Protection (**CBP**), Immigration and Customs Enforcement
- U.S. Department of Justice (**DOJ**)

Significant Penalties for Violations

➤ Civil

- ❖ **ITAR:** Civil penalties of over \$1.16 million per violation
- ❖ **EAR** and **OFAC** sanctions: Civil penalties per violation of ~\$300,000 or twice the amount of the value of the underlying transaction (whichever is higher)
- ❖ Debarment, denial of export privileges, listing on USG denied party lists, blocking of transactions

➤ Criminal

- ❖ **ITAR:** Up to \$1 million per violation for corporations; up to \$1 million per violation and up to 10 years in jail for individuals
- ❖ **EAR** and **OFAC** sanctions: Up to \$1 million per violation for corporations; up to \$1 million and up to 20 years in jail for individuals

Other consequences for violations of the export control and sanctions laws

- Debarment from participation in U.S. government contracts
 - Travel bans
 - Bans from access to the U.S. market (goods, services, financing, etc.)
 - Listing on sanctions lists (meaning that other companies will no longer be permitted to do business with you)
- ***All of these consequences can occur through administrative action with no trial and minimal due process***

Major sanctions and export compliance issues for U.S. and global companies and financial institutions

- Complex regulations
- Very broad agency jurisdiction
- Significant civil and criminal penalties
- Active, multi-agency enforcement
 - OFAC, SEC, DOJ, Customs, Census, Commerce, Homeland Security, etc.
- 5-year statute of limitations
- Successor liability: regardless of transaction form
 - Equity, purchase out of bankruptcy; asset transfer, etc.
- Financial institutions and lenders as enforcement “deputies”

OFAC's Authority Is Broad and Significant

- **Sanctions are not normal financial or trade regulations**
 - These are presidential national emergency powers issued under the authority of the “International Emergency Economic Powers Act” (IEEPA)
 - Sanctions regulations are not subject to notice and comment rulemaking
 - Normally no grandfathering for pre-existing arrangements
 - Strict liability under the civil penalty regime
 - No *de minimis* exceptions — even a donation or humanitarian activity may be prohibited
 - Don't assume that because the sanctioned party is not financially better off that there are no sanctions concerns





Financial institutions take a lead role in enforcement and hold heightened responsibilities under the OFAC sanctions



Financial institutions have mandatory requirements to monitor, block/reject, and report transactions involving sanctioned persons or countries

OFAC Reporting and License Application Forms

Reporting Transactions and Blocked Property to OFAC

- [Report of Blocked Transactions Form](#)  - Please e-mail completed forms to: ofacreport@treasury.gov
- [Report of Rejected Transactions Form](#)  - Please e-mail completed forms to: ofacreport@treasury.gov
- [Guidance on Filing the Annual Report of Blocked Property](#) 
- [Annual Report of Blocked Property Form \(TD F 90-22.50\)](#) 
- [Report a Blocked or Rejected Transaction to OFAC Electronically](#)



OFAC REGULATIONS FOR THE FINANCIAL COMMUNITY

I. Introduction.....	2
II. OFAC Laws, Embargoed Countries, and Criminal Penalties.....	2
III. Civil Penalties	2
IV. Compliance Programs and Audit Procedures.....	2
V. Terminology	3
A—Blocking	3
B—Blocked Account	3
C—General License	4
D—Specific License	4

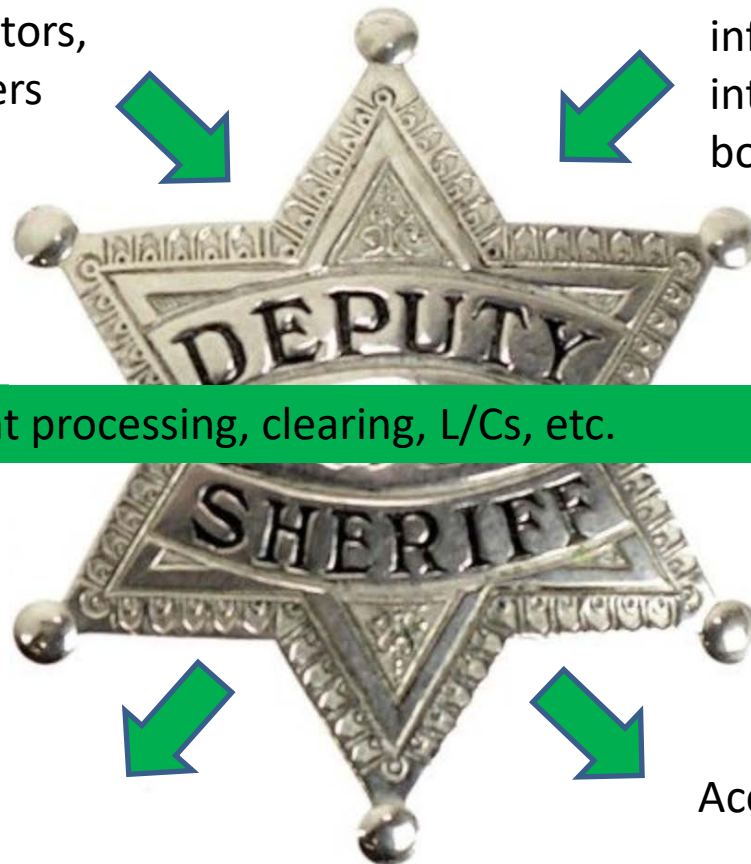
<https://www.treasury.gov/resource-center/sanctions/Pages/regulations.aspx>

Financial institutions are at the crossroads of compliance issues

Investors,
owners



Capital
infusions,
interbank
borrowing



Payment processing, clearing, L/Cs, etc.

Loans,
investments,
leases, secured
transactions,
etc.



Accounts



2. Export Control and Sanctions Law Changes for 2019

Major Changes for 2019


- “Whole of Government” approach to national security concerns regarding China
- Continued tightening of Primary and Secondary Sanctions on Iran
- Re-tightening of sanctions on Cuba
- Updates to list-based and other sanctions on Russia
- Increasing use of data analytics and reporting to detect suspected wrong-doing

Changes to Sanctions & Export Controls on China



The United States is making fundamental changes to the export controls and national security laws regarding China

- These are perhaps the most significant changes in the U.S. export control, national security, and sanctions laws in a generation
- The changes stem from a number of interrelated trade and national security concerns
- The United States is applying a “whole of government” approach with strong bipartisan backing
- Specific initiatives include:
 1. Executive Order 13873 (May 15, 2019)
 2. Entity-specific restrictions
 3. Scrutiny of investments and technology exchanges
 4. New export controls on “emerging and foundational technologies”
 5. Restrictions on telecommunications equipment and services
 6. Heightened enforcement efforts



★ ★ ★

How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World



White House Office of Trade and Manufacturing Policy
June 2018

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY

Daniel R. Coats

Director of National Intelligence

Senate Select Committee on Intelligence

29 JANUARY 2019

China

We assess that China's intelligence services will exploit the openness of American society, especially academia and the scientific community, using a variety of means.

China's Technology Development Strategy

China takes a multifaceted, long-term, whole-of-government approach to foreign technology acquisition and indigenous technology development.



The Entity List

- On May 16, 2019, the United States added Huawei of China and 68 of its overseas affiliates to the “Entity List” (Supplement No. 4 to Part 744 of the EAR)
- As a result, all exports, reexports, and transfers of goods, software, and technology “subject to the EAR” are prohibited to these entities
- Certain limited exceptions for foreign-made items that “incorporate” certain U.S.-origin content
- An additional group of 5 Chinese entities were added last week, joining over 400 other Chinese entities on the list

The Unverified List

- BIS has also continued to add Chinese entities to a list of entities that it has been unable to verify are in full compliance with the EAR
- Supplement No. 6 to Part 744 of the EAR
- Licenses will normally be required and no license exceptions may be used to export, reexport, or transfer items subject to the EAR to these entities
- This action is having a chilling effect on trade with these entities, especially for companies engaging in collaborative research (deemed exports) and other regular business with these entities

Executive Order 13873 (May 15, 2019)

- Prohibits “any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service” that involve “information and communications technology or services designed, developed, manufactured, or supplied, by persons controlled by, or subject to the jurisdiction of a foreign adversary.”
- Widely expected to impact Huawei and other Chinese telecom and IT companies
- Civil and criminal penalties authorized under IEEPA, the same statute that authorizes other U.S. sanctions regulations

Executive Order 13873 (continued)

- Implementing regulations are being developed and are currently set to go into effect no later than October 12, 2019
- Transactions may be prohibited when any one of three conditions is met:
 1. The transaction poses an “undue risk” of sabotage or subversion of “design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States.”
 2. The transaction poses an undue risk of “catastrophic effects” on “the security or resiliency of United States critical infrastructure or the digital economy of the United States.”
 3. The transaction “otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.”

The impact of EO 13873 is likely to be far-reaching

THE WALL STREET JOURNAL.

Nathaniel Bolin ▾

U.S. Edition ▾ | June 25, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business **Tech** Markets Opinion Life & Arts Real Estate WSJ. Magazine

Search 🔍

TECH

U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China

Move follows White House executive order restricting some foreign-made gear and services



Other related restrictions are in the works

- Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (Aug. 13, 2018) requires DoD, GSA, and NASA to issue rules by August 2019 banning Huawei and other named Chinese companies' telecommunications equipment and services from the USG supply chain
- The State of Vermont has adopted a similar rule for state-level procurement, and other states may follow
- The federal rules are in the process of being drafted, and we expect an interim rule to be issued by the August 2019 deadline

New controls on “emerging and foundational technologies”

- Section 1758 of the Export Control Reform Act of 2018 (**ECRA**) requires the U.S. Departments of Commerce, in cooperation with the Departments of State, Energy, and Defense to identify and place new controls on **“emerging and foundational technologies”**
- ECRA was signed into law in August 2018 as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (Aug. 13, 2018)
- Rulemaking to implement ECRA is continuing, but the pace has slowed
- Proposed rules expected later this year

The proposed new U.S. export controls on emerging and foundational technologies may:

- Put **new limits on cross-border R&D and manufacturing** involving AI, data analytics, biotech, robotics, advanced materials, aerospace, and other areas deemed sensitive to U.S. national or economic security
- Further **restrict foreign investment** in U.S. companies and J.V. arrangements with U.S. partners
- **Open opportunities for companies and investors** from countries viewed favorably by U.S. policymakers
- Point the way to **new multilateral controls**

Visa and “deemed export control” restrictions

- The United States continues to restrict new and renewal visas for Chinese persons traveling to the U.S. and working with U.S. companies
- Applications for EAR licenses to engage in transfers of controlled software or technology to Chinese employees in the United States (so-called “deemed exports”) are also being denied with increasing frequency
- As a result, the trend of universities and other research programs cutting ties with Chinese researchers and partners is likely to accelerate

Key points to remember

- ✓ The United States is continuing to aggressively use the export control and sanctions laws to address perceived national security threats regarding China
- ✓ New and potentially very disruptive controls will continue to be added throughout 2019 and beyond at a rapid pace
- ✓ Normally, there is no grace period for implementation and no “grandfathering” of existing commercial arrangements
- ✓ Companies should be acting now to assess the risk to their business and supply chains and to put in place contingency plans

Changes to Sanctions & Export Controls on Iran











 **Donald J. Trump** 
@realDonaldTrump 

12:01 PM - Nov 2, 2018

 101K  62.4K people are talking about this

 **Donald J. Trump**  @realDonaldTrump · Jun 21 

....On Monday they shot down an unmanned drone flying in International Waters. We were cocked & loaded to retaliate last night on 3 different sights when I asked, how many will die. 150 people, sir, was the answer from a General. 10 minutes before the strike I stopped it, not....


 23K  26K  120K

 **Donald J. Trump**   

@realDonaldTrump

....proportionate to shooting down an unmanned drone. I am in no hurry, our Military is rebuilt, new, and ready to go, by far the best in the world. Sanctions are biting & more added last night. Iran can NEVER have Nuclear Weapons, not against the USA, and not against the WORLD!

6:03 AM - 21 Jun 2019

29,403 Retweets 143,657 Likes 

Iran – Changes to U.S. Sanctions after May 8, 2018

- On May 8, 2018, President Trump announced that the United States was withdrawing from the nuclear agreement with Iran (the “Joint Comprehensive Plan of Action” or “JCPOA”) that had gone into effect in January 2016
- As a result, most “secondary sanctions” on non-U.S. persons doing business with Iran snap back into place
- These secondary sanctions are again in full force following “wind-down” periods that expired on August 6th or November 5th (depending on the activities involved)
- The USG is aggressively enforcing these sanctions

The United States Continues to Tighten the Sanctions

- Many non-U.S. companies have announced that they are withdrawing from the Iranian market
- U.S. and non-U.S. financial institutions are now blocking and reporting to OFAC various transactions involving Iran
- These changes are affecting a wide range of companies and industries, including med/pharma, insurance, banking, and IT
- New secondary sanctions on investments in Iran's steel and aluminum sectors were announced in May 2019
- On June 24, 2019, President Trump announced additional sanctions against Iranian government interests and financial institutions facilitating transactions with such interests

Changes to Sanctions & Export Controls on Cuba



Further (Re) Tightening of Cuba Sanctions

- Prohibit transactions with entities listed on the State Department's "Cuba Restricted List" (over 175 entities, including government-owned companies, manufacturers, and hotels)
- June 5, 2019, changes by OFAC and BIS further tightened limited exceptions to the almost total U.S. embargo on Cuba
- Individual and group person-to-person "educational" travel no longer authorized and new restrictions on carriers and vessels
- Exports from outside the United States to Cuba normally not covered by license exceptions and general licenses

State Department List of Cuban Restricted Entities



<https://www.state.gov/cuba-sanctions/cuba-restricted-list/list-of-restricted-entities-and-subentities-associated-with-cuba-as-of-april-24-2019/>

Changes to Sanctions & Export Controls on Russia



Overview of Russia Sanctions

Implemented through a series of Executive Orders beginning in 2014:

- “Traditional” sanctions (E.O. 13660, 13661, 13685)
 - Asset freezes on designated persons and the entities they own
 - Many Russian businessmen with large international holdings who are part of Putin’s “inner circle” have been designated
- Sectoral sanctions (E.O. 13662)
 - More limited sanctions on identified companies in Russia’s financial, energy, and defense sectors.
 - OFAC Directives 1, 2, 3, and 4
 - Sanctions generally target these companies’ access to U.S. oil and gas technology and debt and equity markets

Overview of Russia Sanctions (cont'd)

- EAR Section 746.5 restrictions on certain exports, reexports, and transfers to the Russian oil and gas sector
- ITAR and EAR Section 744.21 restrictions on military end uses and end users in Russia.
- EAR Entity List restrictions on persons, entities, locations in Russia
- Comprehensive embargo on the Crimea region (E.O. 13685)
 - Prohibits new U.S. investment in Crimea and import or export of goods, services or technology to or from Crimea
 - OFAC and Commerce (BIS) may identify and block persons operating in or leading/owning entities in Crimea

Recent Changes to Sanctions and Export Controls on Russia

- On April 6, 2018, OFAC designated additional Russian individuals and entities as sanctioned persons
- As a result, transactions with major Russian companies, including aluminum producer Rusal, became restricted
- OFAC has issued general licenses authorizing some activities with the newly sanctioned persons, and in January 2019 delisted Rusal and a few other companies when their “oligarch” investors relinquished their shares
- OFAC, BIS, and CBP are focusing on enforcement of Russia sectoral sanctions at the border, detaining or seizing shipments
- Banks are increasingly monitoring transactions with listed Russian entities and their subsidiaries
 - OFAC recently announced its first penalty case involving the sales term restrictions in the sectoral sanctions: <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190425.aspx>

Even more Sanctions and Export Controls on Russia

- On August 8, 2018, President Trump invoked the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (CBW Act) in response to the attempted poisoning in Salisbury, UK of Sergei Skripal and his daughter
- On August 27, 2018, the State Department imposed sanctions under the CBW Act, including new limits on exports and reexports of defense articles, defense services, and dual-use items controlled for national security reasons
- While some license exceptions remain and licenses for some activities may be granted on a case-by-case basis, overall, the U.S. is continuing to tighten trade with Russia
- Additional CBW Act sanctions (including import restrictions, additional export controls, restrictions on loans to the Russian government, restrictions on Russian airline flights to the United States, and suspension of diplomatic relations) could follow at a date yet to be specified . . .
- Congress is also considering new legislation that will impose additional sectoral sanctions and export controls on transactions with Russia, Russian banks, and other sectors

Changes to Sanctions and Export Controls on North Korea



Changes to the Sanctions on North Korea

- Under the authority of the Countering America's Adversaries Through Sanctions Act (CAATSA), the U.S. has been imposing additional sanctions on companies doing business with North Korea and North Korean entities
- These sanctions include:
 - Stepped up inspections and seizures of imports suspected of being the product of North Korean inputs or labor
 - Secondary sanctions on persons engaging in certain transactions with North Korea
- While there is little remaining direct U.S. trade with North Korea, these requirements raise the stakes for companies to conduct careful diligence on their supply chains and customer base

New Sanctions on Venezuela



Frequent updates in response to Venezuelan crisis:

- Certain Venezuelan government entities have been on OFAC's SDN List since 2015 – others, such as Petroleos de Venezuela, S.A. (PdVSA) and government officials have been added recently under E.O. 13850
 - Almost all transactions with these entities and their 50% or more owned subsidiaries are prohibited unless authorized by an OFAC general or specific license
- E.O.s 13808, 13827, 13835, 13850, and 13857 also prohibit U.S. persons from dealing in:
 - New debt of the Government of Venezuela (GoV) (other than PdVSA) with a maturity greater than 30 days
 - Bonds issued by the GoV prior to August 24, 2017
 - Digital currency issued by the GoV after January 8, 2019
 - Debt owed to the GoV
 - Certain transactions related to equity interests of entities owned 50% or more by the GoV
- OFAC General Licenses authorize some limited transactions

Venezuela Compliance Best Practices

- Screen daily for involvement of SDNs and their subsidiaries/affiliates
 - do not proceed if SDN involvement is confirmed or seems likely
- Obtain complete end use, end user, and end destination information and screen for possible export control prohibitions, such as military end users
- Where possible, avoid sales terms of net X days and insist on cash payments prior to shipment
- If the transaction involves the GoV, PdVSA (or its affiliates) or the Venezuelan oil and military sectors, assume that it will be prohibited unless a general or specific license applies
- Ensure that customers have notice of and agree to comply with the U.S. sanctions

3. Enforcement Update

Current Enforcement Landscape

- The enforcement of export controls and sanctions violations remains a priority for DOJ, OFAC, BIS, and other law enforcement and regulatory agencies
- DOJ has stated publicly that it will pursue criminal charges against corporate entities and employees for export control and sanctions violations
- Other agencies also have focused on investigating and penalizing large companies and high-ranking employees
- Agencies are cooperating with each other in large investigations and obtaining significant penalties

Current Enforcement Landscape

- The number of export controls and sanctions prosecutions initiated by DOJ is consistent with prior years
- Recent criminal export controls and sanctions cases have focused on Iran and China
 - Criminal enforcement priorities mirror regulatory activity
- Criminal export controls and sanctions cases often involve other charges
 - Trade secrets, economic espionage, etc.
 - Particularly with China

Current Enforcement Landscape

- When is DOJ more likely to become involved in an investigation?
 - Target is a large corporation or high-ranking employees
 - Technology or goods involved are perceived to affect national security
 - Countries involved are a focus of recent regulation
 - Targets are not cooperative, are not providing truthful information, or are obstructing an investigation
 - Potential for other significant federal criminal charges (e.g., trade secrets, FARA, CFAA, money laundering, obstruction)

Current Enforcement Landscape

- Increased number of OFAC and BIS enforcement actions in 2019
- Actions against numerous financial institutions, but also against companies in the engineering, manufacturing, shipping, and software sectors
- Don't overlook exposure for past conduct that violates now-defunct sanctions regimes
- Iran and China are a focus
- Companies can continue to expect greater scrutiny from OFAC and BIS
 - Be mindful of foreign subsidiaries

Current Enforcement Landscape

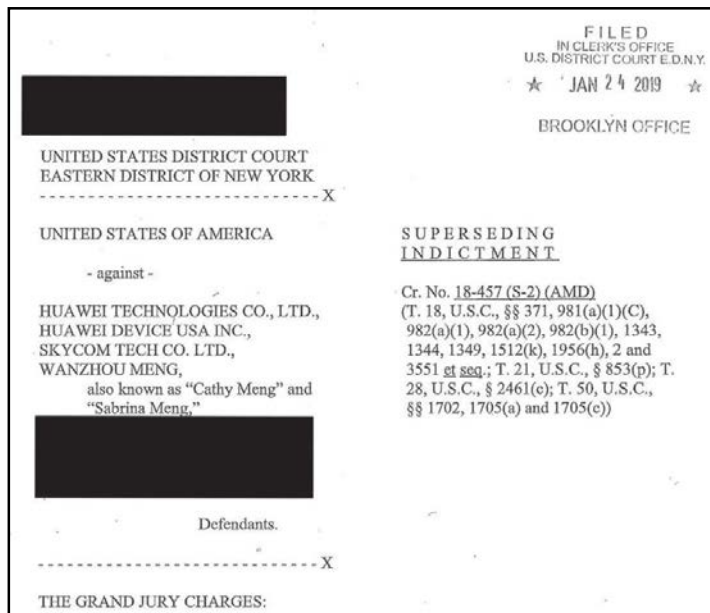
- OFAC’s “Framework for Compliance Commitments” (May 2019)
 - Formally puts companies on notice of OFAC’s expectations with respect to an effective sanctions compliance program
 - Mirrors requirements set forth in the Bank Secrecy Act
 - Issued contemporaneously with DOJ’s guidance on corporate compliance programs (consider both, together)
 - OFAC will take into account whether a company maintains an effective sanctions compliance program in determining whether and what penalties to impose
 - Message is consistent with OFAC’s statements in recent settlements (e.g., Stanley Black & Decker (Mar. 2019))

Current Enforcement Landscape

- OFAC’s “Framework for Compliance Commitments”
 - Five essential components of an effective sanctions compliance program:
 - Management Commitment
 - Risk Assessment
 - Internal Controls
 - Testing and Auditing
 - Training
 - Also identifies the “root causes” of sanctions violations
 - Notable focus on activities and conduct of non-U.S. persons
 - Will heighten OFAC’s expectations with respect to compliance
 - Companies are on notice

Current Enforcement Landscape

- Notable Recent Enforcement Actions:
 - U.S. v. Huawei Technologies Co. Ltd., et al.



Current Enforcement Landscape

▪ Notable Recent Enforcement Actions:

- U.S. v. Huawei Technologies Co. Ltd., et al.
 - 13-count indictment filed in EDNY
 - 4 defendants – Huawei, 2 subsidiaries (U.S. and Iran), CFO
 - Charges include bank fraud, wire fraud, IEEPA, money laundering, obstruction, conspiracy
 - Charges relate to Huawei’s business in Iran
 - Allegations include Huawei’s efforts to obstruct the investigation
 - Subsequent placement of Huawei and dozens of affiliates on the U.S. Department of Commerce “Entity List,” which prohibits purchases of parts and components from U.S. companies without a permit
 - Certain transactions are OK under a general license until Aug. 2019

Current Enforcement Landscape

- Notable Recent Enforcement Actions:
 - Societe Generale SA (Nov. 2018)
 - Global settlement with agreement to pay approximately \$1.34 billion
 - Involves SDNY (DOJ), DANY, OFAC, Federal Reserve, NYDFS
 - Standard Chartered Bank (Apr. 2019)
 - Extends previous DPA
 - Involves DANY, Federal Reserve, NYDFS, UK FCA, DOJ, and OFAC
 - Over \$800 million in combined fines and forfeiture
 - Not voluntarily disclosed
 - UniCredit Group (Apr. 2019)
 - Fines and forfeiture total over \$1.3 billion
 - Guilty plea to criminal IEEPA violation
 - Involves DOJ, OFAC, DANY, NYDFS

Current Enforcement Landscape

▪ DOJ's Voluntary Self-Disclosure Program

- DOJ wants to incentivize companies to voluntarily self-disclose
- Companies should also continue to submit VSDs to the appropriate regulatory agencies
- Consider when a disclosure is “voluntary”
- Company must cooperate fully with the government's investigation
- DOJ will evaluate whether company timely and appropriately remediated issues
- Will not be available if there are “aggravating circumstances”

Current Enforcement Landscape

▪ DOJ's Voluntary Self-Disclosure Program

- Potential Benefits

- Eligibility for a significantly reduced penalty, including the possibility of a non-prosecution agreement, reduced period of supervised compliance, reduced fines/forfeiture, and no monitor

- Whether to voluntarily self-disclose

- If a company chooses not to report, it will lose out on potentially significant reductions in penalties
- VSD likely increases costs and heightens the risk of prosecution
- Must be prepared to cooperate and disclose all relevant information
- Unclear whether DOJ will credit a VSD to another agency

4. Best Practices

Compliance Best Practices

- Work to establish a “culture of compliance,” including an awareness by employees that any criminal conduct will not be tolerated
- Ensure that all corporate affiliates – particularly those located abroad – understand their U.S. export controls and sanctions obligations
- Dedicate sufficient resources to the compliance function
- Ensure that compliance personnel have qualifications and experience to understand and identify risk factors
- Make compliance function independent

Compliance Best Practices

- Perform effective, company-specific risk assessments and tailor compliance program to meet these risks
- Regularly train employees
- Compensate and promote compliance personnel fairly
- Perform regular audits of compliance program
- Design a reporting structure that facilitates identification of compliance issues to senior officials
- Develop capabilities to initiate internal investigations as soon as a violation is uncovered

Responding to an Enforcement Investigation

- Key Questions:
 - Who is conducting the investigation?
 - What triggered the investigation?
 - What is the scope of the investigation?
 - Is the company or its employees a target, subject or witness?
- It is important to try to answer these questions as soon as possible in order to fashion an appropriate response

Responding to an Enforcement Investigation

- Have an effective response policy in place and communicate this policy to all employees
- Once the company is aware of an investigation, it should immediately begin thinking about an internal investigation
 - Identify relevant facts, including bad facts
 - Prevent further violations
 - Lends credibility to the company and its response to an issue
 - Can insulate management / board from complicity
 - But if you do it, do it right

Responding to an Enforcement Investigation

- Strategic and thoughtful engagement with the U.S. Government is key – understand your facts and figure out the best path forward
- Both DOJ and agencies are willing to consider creative solutions and work with companies to avoid worst-case scenarios
 - But this will depend on the facts – not with aggravating circumstances



Nate Bolin

Drinker Biddle & Reath LLP

1500 K Street N.W.

Washington, D.C. 20005

(202) 230-5888

Nate.Bolin@dbr.com

www.dbr.com



Peter Baldwin

Drinker Biddle & Reath LLP

1177 Ave. of the Americas, 41st Floor

New York, NY 10036

(212) 248-3147

Peter.Baldwin@dbr.com

www.dbr.com