

# FENWICK

## **U.S. Trade Controls Master Class:**

Legal Framework, Jurisdictional Reach, & Latest  
Developments (China, Russia, Emerging Tech)

May 3, 2023



# Agenda

1. Legal Framework
2. Jurisdictional Reach
3. Policy & Regulatory Developments
4. Enforcement Trends

**Each Section is 55 minutes, including 45 minutes presentation and 10 minutes of Q&A, with a 20 minute break in the middle.**



Section 1

# Legal Framework

# U.S. History of Trade Controls

- Trade restrictions are part of the American DNA
  - Colonial mercantilism led to the Monroe Doctrine and policy of isolationism, which gave way to interventionism and realization of the U.S. dollar's global power, globalization, and now decoupling
  - Early trade controls were rare and limited to armed conflict – began to change following World War II, North Korea, Cuba



# Early Modern Trade Controls

- The modern era of U.S. trade controls began with World War II – 1940 authority to restrict munitions and civilian goods
- Following end of World War II, Congress began to curtail some authorizations for the President – continued to be authorized, but with definite expiration dates, and used more as an economic tool to manage global inflation and demand for industrial goods
- Late 1940s: the Cold War and containment policy
  - Trade controls shifted focus to national security, defense planning, and technological development
  - Export Control Act in 1949 established foundation for modern regime
  - Was scheduled to expire in 1951, then Korean War happened
  - Multilateral control groups formed to coordinate restrictions of Soviet Union / Eastern Europe and China
- Export Administration Act of 1969 sought to harmonize U.S. controls with allies, liberalize controls away from embargo mentality, and rationalize the process
- Export Administration Act of 1979 further liberalized controls and provided basis for modern-day Export Administration Regulations (EAR)
- After fall of Soviet Union, U.S. export controls shifted focus to nonproliferation of WMDs (nuclear, chemical, biological, missile) through end user and use catch-all controls

# Government Authorities

- Constitution
- Legislation
- Executive Orders
- Regulations
- Policy Statements
- Published Guidance
- Advisory Opinions/Binding Rulings/Licenses



# U.S. Constitutional Basis for Trade Controls

- States cannot regulate foreign trade or make foreign policy
- Congress and President share the foreign affairs powers
- The Constitution prohibits duties on exports:
  - U.S. Constitution, Article I, Section 9, Clause 5: “No Tax or Duty shall be laid on Articles exported from any State.”
  - But limitations on exports of arms and technologies are permissible as quantitative restrictions and regulation of the “privilege” to engage in foreign trade – foreign trade is not a “right”



# Administrative Process

- Congress cannot pass bills of attainder (targeting a specific person)
- Agencies cannot be arbitrary and capricious
- Constitutional due process
- Administrative Procedure Act
  - Notice and comment on rulemaking
  - Transparency and ad hoc communications
  - Publication in Federal Register
  - Confidentiality
  - Foreign affairs exemptions
  
- Nonetheless, the Administration enjoys significant judicial deference on its foreign affairs powers and matters of national security, very difficult to challenge a trade control measure in court





# The Current Regime

## ■ Dual-Use Controls

- Export Control Reform Act of 2018 (ECRA), 50 USC Section 4801 *et seq.*
- Export Administration Regulations (EAR), 15 CFR Part 730 *et seq.*

## ■ Arms Controls

- Arms Export Control Act (AECA), 22 USC Section 2751 *et seq.*
- International Traffic in Arms Regulations (ITAR) 22 CFR Part 120 *et seq.*

## ■ Nuclear Controls

- Atomic Energy Act, 42 USC Section 2011 *et seq.*
- Nuclear Regulatory Commission (equipment and materials), 10 CFR Part 110
- Department of Energy (nuclear technology and assistance), 10 CFR Part 810

## ■ Emergency Authorities (Basis for Sanctions and Some Export Controls)

- International Emergency Economic Powers Act, 50 USC Section 1701 *et seq.*
- Trading with the Enemy Act, 50 USC Section 4301 *et seq.*
- Office of Foreign Assets Control (OFAC) Regulations, 31 CFR Part 500 *et seq.*

# Administration of Dual-Use Export Controls

## U.S. Department of Commerce, Bureau of Industry and Security (BIS)

- Administers the Export Administration Regulations (EAR), Commerce Control List (CCL)
- Regulates commercial software, technology and goods, including use of standard encryption and other IT equipment and tools
- Includes export administration (regulations and policy, licensing) and enforcement
- Also covers the U.S. antiboycott controls



# Administration of Arms Controls

## U.S. Department of State, Directorate of Defense Trade Controls

- Administers the International Traffic in Arms Regulations, the U.S. Munitions List (USML)
- Regulates:
  - Defense articles – military equipment, and related technical data and software
  - Defense services by U.S. persons
  - Foreign brokering of U.S. defense articles and services
  - Foreign military sales fees and commissions



# Administration of Nuclear Controls

## U.S. Department of Energy, National Nuclear Security Administration

- Administers Part 810
- Nuclear technology and foreign assistance by U.S. persons



## U.S. Nuclear Regulatory Commission

- Administers Part 110
- Exports of listed nuclear materials and equipment related to reactors and materials processing



# Administration of Sanctions

## U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC)

- Administers the OFAC Regulations, issued pursuant to IEEPA, TWEA, and other authorities
- The U.S. maintains several sanctions programs, each with different focus and types of restrictions
- Includes overlapping jurisdiction with export controls for embargoed countries



# Commerce Control List

- **Structure**

- 10 Categories
- 5 Commodity Groups
- Numerous Reasons for Control

- **ECCN** – 5-digit code indicating category, commodity group, and control

- **EAR99** – items not regulated under ECCNs on the CCL, but subject to the EAR



**3** = **Electronics**

**A** = **End Items, Equipment, Accessories, Attachments, Parts, Components, and Systems**

**3A001**

# Commerce Control List

## ■ CCL Categories

- 0 = Nuclear materials, facilities, and equipment (and miscellaneous items)
- 1 = Special Materials and Related Equipment, Chemicals, Microorganisms, and Toxins
- 2 = Materials Processing
- 3 = Electronics
- 4 = Computers
- 5 = Telecommunications and Information Security
- 6 = Sensors and Lasers
- 7 = Navigation and Avionics
- 8 = Marine
- 9 = Aerospace and Propulsion

## ■ Commodity Groups

- A – Hardware
- B – Test, inspection & production equipment
- C – Material
- D – Software
- E – Technology

# Key Concepts in U.S. Trade Controls

- **Foreign Availability** – U.S. competitiveness considerations, and evaluation of effectiveness of unilateral controls
- **Specially Designed** – as a result of development, item has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant control, catch-and-release concept
- **Deemed Export** – technology, technical data, know-how, and software source code are “deemed” to have been exported to the home country of a foreign national within the United States (US.. citizens, green card holders, and refugees/asylees are excluded from this)
- **Re-Export** – movement of an item subject to U.S. jurisdiction that is located abroad from one country to another
- **Transfer (In-Country)** – change of end use or end user within the same country abroad
- **Reason to Know** – factual assessment based on totality of circumstances, what an exporter reasonably should know about a transaction
- **Strict Liability** – a violation is a violation, regardless of whether intentional



# Discussion – How the Legal Authorities Work

## ■ Recent examples:

- Russia trade controls
- Emerging technologies advanced notice of proposed rulemaking
- Export control reform process



Section 2

# U.S. Jurisdiction

# The Long Arms of U.S. Trade Control Jurisdiction

Export Controls → things & end use activity

Sanctions → persons & transactions



# Export Control Jurisdiction

## Dual-Use Controls: EAR Part 734

### Section 734.3 – Items Subject to the EAR

1. All items located in the United States
2. All U.S. origin items wherever located
3. Foreign-made items that meet the *de minimis* rule
4. Foreign-made items that meet the foreign direct product rule

# Export Control Jurisdiction

## Dual-Use Controls: EAR Part 734

### Section 734.3 – Items NOT Subject to the EAR

1. Items subject to another agency's exclusive jurisdiction
2. Informational materials, literature, art, film, music
3. Information and software that are:
  - a) Published
  - b) Fundamental research
  - c) Released in academic teaching labs and courses
  - d) Non-proprietary systems descriptions
  - e) Telemetry data for aerospace systems
  - f) Contained in patents

# De Minimis Rule

- **EAR Section 734.4, and Supplement No. 2 to Part 734**
  - Basic concept: foreign-made items containing certain controlled U.S. content are subject to the EAR
  - Thresholds:
    - **No de minimis threshold** – certain supercomputers with U.S. chips, encryption technology, certain aerospace technology, munitions items destined to arms embargoed countries
    - **10% threshold** – for state sponsor of terrorism countries (presently, Cuba, Iran, North Korea and Syria)
    - **25% threshold** – for rest of world (including Russia, Belarus, restricted regions of Ukraine)

# De Minimis Rule

- EAR Section 734.4, and Supplement No. 2 to Part 734
  - **Mechanics** –
    - Identify and combine value of all U.S.-origin controlled content, based on fair market value in country where foreign product is made (actual cost or constructed value)
    - Divide by the value of the foreign product in the market where sold (actual price or constructed value)
    - Software license valuation may be spread across projected sales
    - Software and hardware may be bundled, but not technology
  - **Controlled** – not all U.S.-origin content must be counted, just content that is controlled to the destination country (requires export authorization), controls determined by country only (not Entity List or other end use/user restrictions)
  - **Technology** – before relying on *de minimis* rule to exclude foreign-made technology commingled with controlled U.S.-origin technology, you must file a one-time report with BIS to confirm methodology

# De Minimis Rule

## ■ Sample Case for Discussion

- Industrial machinery made in Sweden by non-U.S. company, has robotic functions and would be controlled under ECCN 2B997 if made in U.S.
- The only U.S.-origin components, which account for 20% of the total finished value, consist of microcontroller chips controlled under ECCN 3A991 and computing equipment controlled under ECCN 4A994.
- The company has received an order to sell the equipment in:
  - Iran
  - China
  - Russia

→ Subject to U.S. jurisdiction under the *de minimis* rule?



# De Minimis Rule

## ECCN 2B997

“Robots” not controlled by 2B007 or 2B207 that are capable of employing feedback information in real-time processing from one or more sensors to generate or modify “programs” or to generate or modify numerical program data

Reason for Control: Anti-Terrorism Column 1

## ECCN 3A991

Electronic devices and “components,” not controlled by 3A001.

Reason for Control: Anti-Terrorism Column 1

## ECCN 4A994

Computers, “electronic assemblies” and related equipment, not controlled by 4A001 or 4A003, and “specially designed” “parts” and “components” therefor (see List of Items Controlled).

Reason for Control: Anti-Terrorism Column 1

# De Minimis Rule

Countries	Chemical and biological weapons			Nuclear nonproliferation		National security		Missile tech	Regional stability		Firearms	Crime control			Anti-terrorism	
	CB 1	CB 2	CB 3	NP 1	NP 2	NS 1	NS 2	MT 1	RS 1	RS 2	FC 1	CC 1	CC 2	CC 3	AT 1	AT 2

Iran: U.S. embargo, all items listed on the CCL (EAR Part 746)

China: no X in the box for anti-terrorism

Russia: no X in the box for anti-terrorism ... but Russia trade restrictions on all items listed on the CCL (EAR Part 746)

# Foreign Direct Product Rule

- Section 734.9 -- the advanced part of the EAR, not for the faint at heart
  - **The concept:** Foreign-produced items located outside the United States are subject to the EAR when they are a direct product of specified technology or software, or are produced by a plant or major component of a plant that itself is a direct product of specified technology or software.
  - **Definitions**
    - ***Direct product:*** The immediate product (including processes and services) produced directly by the use of technology or software.
    - ***Equipment:*** This is a combination of parts, components, accessories, attachments, firmware, or software that operate together to perform a function of, as, or for an end item or system. Equipment may be a subset of end items based on the characteristics of the equipment.
    - ***Major Component :*** A major component of a plant located outside the United States means equipment that is essential to the production of an item, including testing equipment.
    - ***Production:*** Means all production stages, such as: product engineering, manufacture, integration, assembly (mounting), inspection, testing, quality assurance.

# Foreign Direct Product Rule

- The many versions of the Foreign Direct Product Rule
  - The “classic” – national security version
  - The munitions and space versions
  - The Entity List version (started with Huawei, expanded to other listed parties in China with footnote by their name)
  - The Belarus/Russia version
  - The Belarus/Russia military version

## Foreign Direct Product Rule

- Discussion example: turning back to our robotics case, now let's assume that the equipment is made with production machinery that is itself controlled under various ECCNs in Category 2

# Export controls: What is a U.S. Person?

- Export controls limit the ability of U.S. persons to “support” certain prohibited end uses.
  - U.S. citizen
  - U.S. lawful permanent resident (*i.e.* Green Card Holder)
  - Certain protected persons (*i.e.*, asylees and refugees)
- Export controls also impose limits on transfers of sensitive technical data and software to foreign nationals
  - U.S. person dual nationals are always considered U.S. persons
  - In cases of dual/third country nationals, generally look to most recently acquired nationality, also substantive contacts with other nationality
  - Persons located in the United States on a temporary terms (*e.g.*, work, tourist, student, diplomatic, investor visa) are NOT U.S. persons



# Sanctions: What Is a U.S. Person?

## ■ Sanctions

- U.S. citizen or lawful permanent resident (*i.e.*, Green Card holder)
- Any person located in the United States (including temporary foreign visitors)
- Any company organized under U.S. law and its unincorporated branches, officers, or operations abroad
- In the case of Cuba and Iran sanctions, and foreign incorporated entity that is owned or controlled by U.S. persons



# Common sanctions jurisdictional touch points

- In addition to U.S. persons, non-U.S. persons must comply with U.S. sanctions when their activities directly or indirectly involve the United States or U.S. persons
- Result is that much commerce outside of the United States is ultimately subject to U.S. “primary” sanctions jurisdiction
- Common examples:
  - Use of US Dollars or other indirect use of the U.S. financial system
  - Use of US IT systems or networks
  - Use of personnel in the United States or U.S. person personnel abroad
  - Ordering services or products from the United States
  - Back-office support from the United States
  - In some cases, shipments of U.S. goods



# Key sanctions jurisdiction concepts

- **Causation:** Non-U.S. persons violate U.S. sanctions if they knowingly “cause” a U.S. person to conduct a transaction that violates U.S. sanctions laws.
  - Classic example is the bank stripping cases where foreign banks removed references to sanctioned countries and persons before passing transactions through their U.S. correspondent accounts
  - A violation occurs even if the U.S. person does not know that sanctioned regions or persons are involved
  
- **Facilitation:** A U.S. person may not assist or “facilitate” a transaction between non-U.S. persons that the U.S. person could not conduct directly themselves.
  - Common examples:
    - Approving a transaction
    - Referring business to a foreign affiliate
    - Changing procedures to allow a foreign affiliate to do business with a sanctioned party or region
    - Providing engineering or IT support
  - Does not include passive receipt of data; U.S. sanctions compliance guidance

# Secondary sanctions

- “Secondary” sanctions authorize the U.S. government to impose economic consequences non-U.S. companies for conduct that occurs wholly outside of the United States and threatens U.S. interests
- Not formal prohibitions
- Non-U.S. companies do not “violate” U.S. law if they contravene a secondary sanction, but do risk potentially becoming sanctioned themselves
- Two typical examples:
  - Congressionally imposed secondary sanctions (e.g., CAATSA 228)
  - “Material assistance” designation authorities
- Exercise of secondary sanctions authorities can be geopolitically sensitive

# Exemptions and general licenses

- Certain activities are generally exempt from U.S. sanctions laws, including certain activities related to:
  - Personal communications
  - Humanitarian donations
  - Informational materials
  - Travel (but not in the Cuba context)
  - *Caution:* these exemptions are construed narrowly. Most business related activities are not covered by these exemptions.
  
- OFAC also generally authorizes (allows) U.S. persons to engage in limited activities involving sanctioned countries or persons that support U.S. policy goals, including certain activities related to:
  - Personal communications over the internet
  - Telecommunications
  - Personal remittances
  - NGO activities
  - Food, medicine, and medical devices

# Export Controls & Sanctions Overlap

Discussion –

Overlap between export controls and sanctions jurisdiction, and “sanctionization” of export controls:

- U.S. person concept increasingly used in export controls
- Expanded use of list-based export restrictions, like Entity List
- Defense trade controls cover services and brokering
- Sanctions implementation of embargoes can cover exports/re-exports of things
- Software-as-a-service – export controls apply to data transfers and software downloads, and sanctions apply to the service aspect

Section 3

# Policy & Regulatory Developments

# Russia & Belarus

- **Broad trade controls, not an embargo, but getting closer**
  - All items with an ECCN on the CCL, including unilateral controls that go beyond EU's Dual-Use list
  - Industry sector sanctions, several lists covering EAR99 items, targeting the following:
    - Energy sector
    - Luxury goods
    - Industrial items
    - Items of low availability and critical significance to Russian economy
    - Chemical weapons precursors
  - Total ban on military end use, many parties on Entity List
  - Far-reaching jurisdictional rules



# Russia & Belarus



## ■ Differences between US and EU regimes

- U.S. administers Russia trade controls through a combination of BIS (export controls), DDTC (defense trade), and OFAC (sanctions)
  - They operate in conjunction but have wholly separate jurisdictions, restrict different aspects of a transaction
  - Multiple government authorizations may be required
- U.S. government issues many general licenses / license exceptions, and can be flexible on scope of specific licenses
- But, processing times are longer
- U.S. government won't grant comfort letters or assurances, but can engage in informal dialog

# Russia & Belarus

- **More differences between US and EU regimes**
  - EU “technical assistance” and “making available” concepts do not have exact parallels under U.S. dual-use controls, but
    - General Prohibition 10 for items illegally exported
    - Comprehensive support ban for denied persons list
    - Restrictions on technology transfers
    - Restrictions on defense services
  - More similar to U.S. sanctions concept of facilitation, but that applies to persons and transactions, not linked to export controlled items
  - U.S. makes up for this in our far-reaching export controls around re-exports and in-country transfers



# Russia & Belarus

## ■ What's Next?

- We are watching the mid-May G-7 meeting in Japan
- U.S. has proposed a comprehensive embargo on Russia to expedite a resolution to the conflict
- Pushback reported from Japan and EU
- Likely some compromise will emerge, with tightening of controls to address backfill, including coordination on China
- U.S. government also has emphasized increased focus on export control and sanctions enforcement of existing controls and circumvention by non-U.S. companies

# China

## ■ Latest Trade Control Developments

- Fall 2022 – advanced chip and semiconductor export control rule – and China’s challenge at the WTO (symbolic move)
- Continued addition of Chinese parties to the Entity List
- China tariffs remain untouched



# China

## ■ Recent Political and Economic Events

- The balloon flyover
- Taiwan tensions (China drone flyover and warships circling, US naval aircraft transit strait, Taiwan leader visit to US)
- China leaning in towards Russia and visit by President Xi to President Putin (“no-limits friendship”), but also recent call with President Zelensky of Ukraine
- EU leaning harder on China (EU President von der Leyen’s speech last month)
- Latest trade figures show that two-way trade between the US and China set a new record in 2022 - \$690B. Imports from China increased to \$538B in 2022, only slightly less than 2018 when tariffs started. Still largest US trading partner



# China: U.S. Policy Position



- Treasury Secretary Yellen speech
- National Security Advisor Sullivan speech
- Congressional legislation re: TikTok, other issues
- Reported shift in Administration's approach on export licensing for Huawei, and recent Seagate enforcement action, but also no formal statement or official change in position
- CFIUS remains robust for China and tech/personal data

# China

## ■ What's Next

- Outbound investment review
- Tiktok
- Strategic investment in U.S. critical industries and supply chain – semiconductors, clean technology, defense innovation
- Battle over batteries
- Closer U.S. alignment with EU and other allies, as China leans into Russia

# China

## ■ Difficult Issues For Companies in the Path Forward

- Decoupling of trade relationship with China not feasible –
  - China has bigger global footprint and supply chain integration than Russia
- Taller fences and smaller yards on trade controls –
  - Engagement with regulators to avoid restricting mature technologies and impeding cross-border collaboration, or risk U.S. touchpoints being designed-out
- Complexity of U.S. export controls against China –
  - very hard to understand, causing companies with U.S. jurisdictional nexus to de-risk, but also blowback under China's anti-sanctions blocking law, and difficulties with in-country due diligence and end use assurance
- Lack of multilateralism –
  - U.S. hasn't coordinated with allies, U.S. is unique with its Entity List, far reach of U.S. export jurisdiction creates competing demands and risks for non-U.S. companies

# Emerging Technologies Controls

- ECRA Section 1758 obligates BIS to identify and control emerging and foundational technologies significant to national security
- Parallel legislation updated the U.S. Committee on Foreign Investment in the United States (CFIUS) process to include a review trigger for emerging technologies
- BIS Advance Notice of Proposed Rulemaking in 2018
  - BIS has stated that it does not intend to issue an official definition of “emerging technologies” or a final rule to comprehensively complete that rulemaking
  - Rather, issuing piece-meal rules based on initial feedback collected in that process

# Emerging Technologies Controls – 2022 White House Update

- Advanced Computing
- Advanced Engineering Materials
- Advanced Gas Turbine Engine Technologies
- Advanced Manufacturing
- Advanced and Networked Sensing and Signature Management
- Advanced Nuclear Energy Technologies
- Artificial Intelligence
- Autonomous Systems and Robotics
- Biotechnologies
- Communication and Networking Technologies
- Directed Energy
- Financial Technologies
- Human-Machine Interfaces
- Hypersonics
- Networked Sensors and Sensing
- Quantum Information Technologies
- Renewable Energy Generation and Storage
- Semiconductors and Microelectronics
- Space Technologies and Systems



## *CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE*



# Emerging Technologies Controls

- Examples of new controls issued or in rulemaking process for emerging technologies:
  - Geospatial satellite imaging AI software (ECCN 0D521 process)
  - Semiconductors: two substrates of ultra-wide bandgap semiconductors: Gallium Oxide ( $\text{Ga}_2\text{O}_3$ ), and diamond; Electronic Computer-Aided Design (ECAD) software specially designed for the development of integrated circuits with Gate-All Around Field-Effect Transistor (GAAFET) structure
  - Gas turbine engines: Pressure Gain Combustion (PGC) technology
  - Brain control interface technology
  - Gene editing tools and software

# Examples of implemented emerging tech controls

- ECCN 3A001.b.3.f (certain microwave transistors, a major component of wideband semiconductors)
- ECCN 3D005 (continuity of operation software)
- ECCN 5A002.a.4 (postquantum cryptographic algorithms)
- ECCN 6A001.a.1.b.1; .a.2; .a.2.a; .a.2.a.6 (underwater transducers designed to operate as hydrophones)
- ECCN 9A004.g (aircraft platforms specially designed or modified to be air-launch platforms)
- ECCN 2B001.a, .b or .c (hybrid additive manufacturing/computer numerically controlled tools)
- ECCN 3D003 (computational lithography software designed for the fabrication of extreme ultraviolet masks)
- ECCN 3E004 (technology for finishing wafers for 5nm production)
- ECCN 5A004.b (forensics tools that circumvent authentication or authorization controls on a computer and extract raw data)
- ECCN 5D001.e (software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface)
- ECCN 9A004.h, 9A515.a (sub-orbital craft) 12-35) ECCN 1C350.d (24 chemical weapons precursors)
- ECCN 2B352.b.2.b (single-use biological cultivation chambers with rigid walls)
- ECCN 0D521 (software related to analysis of geospatial imagery) [Unilateral]
- ECCN 2D352 (Software designed for nucleic acid assemblers and synthesizers)
- ECCN 1C351.d. (the synthesis and collection of four marine toxins (brevetoxin, gonyautoxin, nodularin and palytoxin))

Section 4

# Enforcement Trends

# U.S Enforcement Framework

- Criminal prosecution, with criminal fines of \$1 million per violation and/or 20 years in prison
- Civil Penalties
  - The maximum civil penalty amount is over \$350K or twice the value of the transaction, whichever is higher
  - Calculated per violation, can translate into \$millions where there are multiple prohibited transactions
- Compliance monitors and mandated audits/reporting
- Loss of export privileges
- Published notice: name-and-shame

# Voluntary Self-Disclosure Concept

- U.S. Enforcement Guidelines – BIS and OFAC
- New BIS position on failure to file VSD as an aggravating factor (versus just neutral, with mitigation for choosing to file)
- The vast majority of VSDs resolve with a private warning letter

# Recent Cases

## ■ Seagate

- Exports to Huawei in violation of the foreign direct product (FDP) rule
- Seagate had HDD manufacturing sites in China, Northern Ireland, Malaysia, Singapore, Thailand, and the United States. Seagate used equipment, including testing equipment, subject to the EAR and the FDP rule
- After the Huawei FDP rule was imposed, Seagate announced it would continue to do business with Huawei despite the fact that its only two competitors had stopped selling HDDs to Huawei, resulting in Seagate becoming Huawei's sole source provider of HDDs
- Seagate sold over \$1B of HDD items to Huawei
- Penalties of \$300B, mandatory audits, suspended denial order

# Recent Cases

## ■ Microsoft

- Microsoft sold software licenses, activated software licenses, and/or provided related services from servers and systems located in the United States and Ireland to SDNs, blocked persons, and other end users located in Cuba, Iran, Syria, Russia, and the Crimea region of Ukraine
- Microsoft Entities engaged with third-party distributors and resellers to sell Microsoft software products
- Process involved U.S.-based servers and systems managed by personnel in the United States or third countries
- Violations caused by the lack of complete or accurate information on the identities of the end customers for Microsoft's products
- Russia entity employees put inaccurate information into the sanctions screening system
- During the time period in which the apparent violations occurred, Microsoft did not screen for SDN ownership or for SDNs' using native scripts
- Combined penalty of over \$3M – BIS and OFAC

# Recent Cases

## ■ British American Tobacco (BAT)

- DOJ / OFAC joint enforcement - \$629 million
- BAT's violations arose from its formation of a conspiracy to export tobacco and related products to North Korea and receive payment for those exports through the U.S. financial system and from its subsidiary's use of U.S. financial institutions to receive or otherwise process U.S. dollar-denominated (USD) payments for its sale of cigarettes to the DPRK Embassy in Singapore.
- In doing so, BAT caused U.S. financial institutions to process wire transfers that contained the blocked property interests of sanctioned North Korean banks and to export financial services and facilitate the exportation of tobacco to North Korea.
- BAT's Standing Committee, which included BAT's top executives in London, approved a scheme to create the illusion of distance between the company and North Korea.
- BAT and its subsidiaries sought to conceal their conduct from banks, for example by letting wire transfers expire rather than respond to questions from a bank that would have revealed the payment's connection to North Korea.
- Without a culture of compliance driven by senior management and attendant policies and controls, firms increase the risk that they may engage in apparently violative conduct.



# Recent Cases

## ■ SAP

- SAP sold software licenses and maintenance services to resellers located in Turkey, the United Arab Emirates, Germany and Malaysia, which in turn sold the licenses and services to third parties for end use in Iran. Iranian end users then downloaded SAP software, updates or patches from the company's servers in the U.S.
- SAP failed to prevent downloads of its software from IP addresses associated with Iran, even though internal audits recommended the adoption of IP address geolocation screening
- Appropriate due diligence, controls, and monitoring of distributors and resellers is a must in any industry, particularly when a U.S. company does not have full insight into the identity of the end users of its goods or services
- SAP allowed its subsidiaries to operate independently, although SAP knew, based on pre- and post-acquisition due diligence, and notification by SAP's U.S. compliance team, that those subsidiaries had insufficient sanctions compliance programs
- Over \$8 million combined DOJ, OFAC, and BIS settlement

# Major Themes and Lessons Learned

- Voluntary self-disclosure is still worth it –
  - significant reduction in penalties compared to non-disclosed cases
  - Most published penalties are issued for non-disclosed cases
- Indications of willfulness, choice not to comply or implement appropriate risk-based controls
- U.S. regulators are focusing on tech sector, software-as-a-service, digital assets and fintech
- Expectation to use what information you're already collecting for compliance screening and diligence

# Red Flags

- U.S. is increasingly focused on red flags, circumvention, and diligence
- Examples of red flags:
  - New customer, no online presence, with questionable credentials
  - Customer located in or closely linked with sanctioned country, or provides inconsistent/evasive information about location
  - “Front companies” with no discernible ownership (e.g., suspected Russian ties, but ownership trail stops cold with a Swiss “foundation”)
  - Customer is reluctant/evasive in providing identification or corporate ownership documents or completing diligence
  - Requests for non-market/standard payment terms
  - Banking institutions located in sanctioned countries
  - Customer with export-banned affiliates wants to download or use software
  - Any indication of fraud or corruption