2019 YEAR-END REVIEW
of Import/Export Developments

Export Controls and Economic Sanctions

Wednesday, November 13, 2019 | Santa Clara, CA & Webcast
Welcome and Introduction
# Agenda

## United States Export Control Developments

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Emerging and Foundational Technologies: Update on the Status of the Regulatory Process</td>
</tr>
<tr>
<td>2</td>
<td>Update on Encryption Regulations</td>
</tr>
<tr>
<td>3</td>
<td>Entity List Developments: Huawei and Others</td>
</tr>
<tr>
<td>4</td>
<td>Changing Export Control and Licensing Policies for China</td>
</tr>
<tr>
<td>5</td>
<td>Export Control and Human Rights</td>
</tr>
</tbody>
</table>
Update on ECRA and Emerging & Foundational Technologies
Emerging & Foundational Technologies (i)

Regulatory Update

• Section 1758 of Export Control Reform Act of 2018 mandated new controls on emerging and foundational technologies

• BIS issued ANPRM about emerging technologies in Nov. 2018, with public comments due in Jan. 2019

<table>
<thead>
<tr>
<th>Biotechnology</th>
<th>Artificial intelligence/machine learning</th>
<th>Position, navigation, and timing technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microprocessor technology</td>
<td>Advanced computing technology</td>
<td>Data analytics technology</td>
</tr>
<tr>
<td>Quantum information and sensing technology</td>
<td>Logistics technology</td>
<td>Additive manufacturing</td>
</tr>
<tr>
<td>Robotics</td>
<td>Brain-computer interfaces</td>
<td>Advanced materials</td>
</tr>
<tr>
<td>Hypersonics</td>
<td></td>
<td>Advanced surveillance technology</td>
</tr>
</tbody>
</table>
Emerging & Foundational Technologies (ii)

Regulatory Update

- BIS received 231 substantive comments about emerging technologies
- Themes of public comments:

| National security threat needs to be defined | Avoid overlapping with existing controls |
| Narrowly tailored controls should be used   | Exceptions/exemptions needed            |
| Multilateral controls are preferred         | Avoid harm to US economy/tech leadership |

- BIS still working on emerging technology controls; press reports indicate first round of controls may be published by year end
- ANPRM about foundational technologies is still forthcoming
- Status of Emerging Technology Technical Advisory Committee
Encryption Controls
Encryption Controls

Reminder of Framework

- Publicly available?
- Decontrol notes?
- ECCNs
  - 5A002.a – "information security" systems, equipment and "components" – **Primary function test**
    - a.1 information security
    - a.2 digital communication or networking
    - a.3 computing, information storage/processing
    - a.4 crypto supports non-primary function, but performed by incorporated items that would, by themselves, be 5A002/3/4, 5B002/5D002
  - 5A003 – non-cryptographic "information security"
  - 5A004 – systems, equipment and components for defeating, weakening, or bypassing security (cryptanalytic)
- Note 3: Mass-market 5X992.c (not for ENC (b)(3)(iii); (b)3) requires BIS classification; (b)(1) self-classifiable with annual self-classification report
- License Exception ENC:
  - 740.17(a) – no submissions/reporting required
  - 740.17(b)(2) or (b)(3)(iii) – Classification request required + semi-annual sales report; may require specific license for gov't end-users ex-Supp 3
  - 740.17(b)(3)(i)(ii) or (iv) – Classification request
  - 740.17(b)(1) – self-classification + annual self-classification report
- **Feb 1, 2020: Next annual self-classification reporting deadline**
Entity List
Developments and Mitigation Strategies
## Entity List – Recent Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 30, 2018</td>
<td>Fujian Jinhua Integrated Circuit Company (JHICC) added (DRAMs)</td>
</tr>
<tr>
<td>May 16, 2019</td>
<td>Huawei + 68 affiliates added</td>
</tr>
<tr>
<td>May 20, 2019</td>
<td>Huawei – 90 day Temporary General License authorizing limited transactions</td>
</tr>
<tr>
<td>June 27, 2019</td>
<td>Five Chinese entities associated with supercomputer development (inc. Sugon, Higon, Wuxi Jiangnan ICT)</td>
</tr>
<tr>
<td>Aug 19, 2019</td>
<td>Huawei Temporary General License revised and extended to Nov 18, 2019, 46 more Huawei entities added</td>
</tr>
<tr>
<td>Sep 9, 2019</td>
<td>BIS FAQs on Huawei Entity Listing and TGL</td>
</tr>
<tr>
<td>Oct 14, 2019</td>
<td>Dahua, Hikvision + 26 other Chinese entities – for human rights abuses</td>
</tr>
</tbody>
</table>
Key Entity List Considerations (i)

- Not same as other restricted parties lists
- Transaction must involve item subject to EAR
- Applies to any person exporting, reexporting, transferring items subject to EAR, not just US persons

Normal *de minimis* rules apply – apply thresholds based on destination (*de minimis* rules are not end use/end user based)

- May not always apply to all items subject to EAR
- If you receive items, can you send them back? e.g. repair, testing, etc.
Key Entity List Considerations (ii)

- Not triggered by negotiations/contracts/dealings but rather export, reexport, transfer
  - Passage of title/ownership to party already in possession of item is not an export/reexport/transfer subject to EAR with few exceptions (e.g., spacecraft)

- May not always be subject to policy of presumption of denial

- Only applies to listed entities and not unlisted affiliates or subsidiaries BUT:
  - Risk of diversion?
  - Third party acting as agent or intermediary?
### Key Entity List Considerations (iii)

<table>
<thead>
<tr>
<th>Screening challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Same name, same location/address?</td>
</tr>
<tr>
<td>Usually no wind-down periods</td>
</tr>
<tr>
<td>- Limited Huawei temporary general license is somewhat unique</td>
</tr>
<tr>
<td>Some contract sanctity (if already on boat/plane when listing occurs)</td>
</tr>
<tr>
<td>BIS Entity List FAQs</td>
</tr>
</tbody>
</table>
De Minimis Refresher

- Only count content that is controlled to the destination, not end-user
  - e.g., EAR99 content not controlled to China
- No commingling ("apples to apples") unless bundling rule applies
- Is the US content "incorporated"?
- How to calculate US code content?
- Special encryption *de minimis* qualification requirements – EAR 734.4(b)
United States Extraterritorial Export Control Jurisdiction

The "Direct Product" Rule

- Section 734.3(a)(4) of the Export Administration Regulations extends United States export control jurisdiction to certain foreign made direct products of U.S. origin technology (the "direct product rule")
- The following three conditions apply with respect to the direct product rule
  - Is the foreign made product the "direct product" of U.S. origin technology
    - The "direct product" is defined in section 734.3(a)(4) as the "immediate product produced directly by the use of technology or software".
    - Examples of the distinction between (i) a direct product; and (ii) an indirect product, for export control purposes may be found in October 1988 proposed technical data regulations, 53 Fed. Reg. 40074 (October 13, 1988)
  - Was the technology subject to a written assurance requirement when originally exported from the United States, either as a condition of license exception TSR under section 740.6 of the Export Administration Regulations; or as a supporting document for export license to export the technology to a Country Group D destination, under Paragraph (o)(3)(i) of Supplement No. 2 to Part 748 of the Export Administration Regulations.
    - In effect, is the technology subject to national security (NS) controls
  - Is the foreign made product classified under an ECCN that is controlled for national security (NS) reasons
Huawei Entity List Order

Export Compliance Challenges

- Temporary General License: Certification Statement
- Export License Applications: End-Use/End-User Statement
- Technical Support for Foreign Products not subject to the EAR
  - U.S. companies that have determined that certain commodities are not subject to the EAR, and can be lawfully sold and supplied to Huawei
- Renewals of Existing Technology and Software License Agreements
  - Is the renewal limited solely to the receipt of money and the issuance of a license certificate?
  - Issuance of access credentials, software code, license keys, technical assistance or other deliverables
- U.S. Person requesting technical support for installed Huawei products
  - The request for technical support and assistance may disclose or involve the transfer of technology from the United State to Huawei
- Furnishing Technical Assistance or Support for Products running on Huawei Equipment at a Third Party Customer's Site
  - Terms of the Temporary General License (if renewed)
  - Restrictions on interactions with Huawei personnel where the customer has a managed services agreement with Huawei
  - Diagnosis of performance problems as between the U.S. vendor's product and the Huawei equipment
  - Confirmation with the customer that products and related technologies will not be disclosed or transferred to Huawei
- Product certification as to compatibility and interoperability
- Returns of Huawei products under warranty
"Supply Chain" Executive Order

EO 13873 Securing the Information and Communications Technology and Services Supply Chain

• Not specific to Huawei or China per se
• Applies to US persons – OFAC type prohibitions
• Prohibition on acquisition, import, transfer, installation, dealing in, or use:
  • of ICT/S designed, developed, manufactured or supplied by a foreign adversary target or in a transaction involving property interests of a foreign adversary
  • where poses undue risk of sabotage to or subversion of ICT/S in US; undue risk of catastrophic effects on security/resiliency of US critical infrastructure or digital economy; or otherwise unacceptable risk to US national security and security or safety of US persons
• Implementing rules were due by Oct 12th
Federal Procurement Ban

NDAA 889

- **(a)(1)(A) Direct Ban**: Ban on federal agencies procuring, obtaining, extending or renewing contracts to procure or obtain, any equipment, system or service that "uses" "covered telecommunications equipment and services and certain video surveillance equipment" as a *substantial or essential component or as a critical technology part of system*
  - Effective Aug 13, 2019
  - "substantial or essential component" = necessary for proper function or performance of equipment, system or service
  - "critical technologies" = defense articles and services, CCL-controlled items, nuclear materials, toxins, emerging and foundational technologies controlled under ECRA
  - "use"?

- **(a)(1)(B) Indirect Ban**: Ban on federal contracting with *any entity that "uses" any equipment, system or service that "uses" covered equipment and services*
  - Dec 2019 NPRM on indirect ban?
China

Changing US Export Control and Licensing Policies

- Denial of export licenses for (1) 3E002 microprocessor technology to China and (2) for 5E002 technology for use in semiconductor devices in China where SC technology is decontrolled to 3E991/EAR99
- DoD concerns over exports of semi-conductor technology for use in 5G products
- Deemed export license application denials, delays & scrutiny for Chinese nationals
- ECRA 1759 – mandates review of export controls and licensing policies for countries subject to US arms embargoes, aka China
- EAR 744.21 – military catch-all (knowingly/is informed test)
  - Currently limited to military end-uses; possible expansion to end-users?
  - Additional ECCNs to be added to list of items in Supp 2 to Part 744?
- EAR 742.4(b)(7) – NS controls: general policy of approval unless transfer would make a significant contribution to Chinese military capabilities – possible change to case-by-case review? presumption of denial?
- Additional controls on items not currently controlled? e.g. emerging & foundational technologies; semiconductor manufacturing tools (ECCN 3B991)
- License Exception CIV/RPL – possible elimination for China?
5 Export Controls and Human Rights
Draft State Department Guidance on Exports of Items with Surveillance Capabilities

Published 4 September 2019; public comments accepted until 4 October 2019

Guidance does not constitute new export controls or mandatory steps, but focuses on:

- Encouraging exporters to assist in minimizing risk of human rights abuses and other misuse of such items
- Possible due diligence steps and red flag considerations
- Suggested contractual and procedural safeguards to mitigate possible abuse

Perhaps another effort to close perceived "gap" in current export controls

- Possible that many such items are not currently listed on Commerce Control List or are listed but do not require an export license but, nonetheless, can present human rights abuse concerns
Agenda

CFIUS Developments

1. Committee on Foreign Investment in the United States (CFIUS)
2. CFIUS Legislation
3. Critical Technologies Pilot Program
4. Proposed Rules — Apply by February 2020
5. Enforcement
6. Key Themes
Increasing regulation of cross-border investment across advanced markets

- Prompted by Chinese investment, effects are broader.
- Scrutiny amidst interdependence and vulnerability.
- Increasing cooperation among regulators.

US law fundamentally constant since 1988, but broader effect and closer scrutiny

- President has broad authority to intervene in transactions to protect national security.
- New authority to require pre-closing declarations.

Assisted by the Committee on Foreign Investment in the United States (CFIUS)

- Chaired by the US Department of the Treasury.
CFIUS Legislation

President may block a transaction or force divestiture where a foreign person acquires "control" of a US business and the President finds a threat to national security

- Parties may seek clearance of a transaction by the Committee on Foreign Investment in the United States, insulating the deal from subsequent review
- "Control" is any ability to influence business decisions — low bar
- "National security" is undefined, Presidential determinations not subject to judicial review

FIRRMA

- Authorized expanded jurisdiction for technology, infrastructure and data (TID) businesses
  - Board rights, access to nonpublic technical information and substantive decision-making involvement
- Authorized pre-closing mandatory declarations for TID businesses
  - Penalties up to value of investment
  - Filing fees for notifications (not declarations) — capped at 1% of transaction value or $300,000
- Specific provisions for fund investment — conditions for limited partners not to trigger declarations
Critical Technologies Pilot Program

- Mandatory declaration for investments in certain critical technology businesses
  - Pilot Program business
    - US business
    - Develop, test or produce
    - Critical technology — defined by export controls and other regulatory programs
    - Used in/designed specifically for one of 27 listed industries (mostly manufacturing)
  - Pilot Program rights — control, board, information access, substantive decision-making involvement

- Timing: 45 days prior to closing of transaction; decision 30 days after acceptance

- Provisions on funds investments

- Outcomes: clearance, no action or required notice

- Noncompliance consequences: divestiture order, penalty up to value of investment
Proposed Rules — Apply by February 2020

- Jurisdiction expanded to technology, infrastructure and data (TID) businesses as required by FIRRMA
- Scope
  - Technology — undecided, CFIUS considering what to do with Pilot Program
  - Infrastructure — applies to listed types of infrastructure
  - Personal data — scope turning on information sources (e.g., government personnel), types (e.g., biometric) and volume
- Declarations only where a foreign investor acquires a substantial interest (25% or more) in a TID business, and a foreign government has a substantial interest (49% or more) in the foreign person
- Exclusions for "excepted investors" from excepted foreign states designated by Treasury — likely to be very limited
- Maintains jurisdiction provisions on funds — relevance will depend on scope of declaration requirements
Enforcement

- **Prohibitions** — 3 recent Presidential decisions — parties usually withdraw on learning of opposition
  - Broadcom/Qualcomm — Trump, 2018
  - Canyon Bridge/Lattice Semiconductor — Trump, 2017
  - Grand Chip/Aixtron — Obama, 2016

- **Divestiture orders**
  - Beijing Kunlun Tech/Grindr — Trump, 2019
  - iCarbonX/PatientsLikeMe — Trump, 2019
  - HNA/850 Third Ave — Trump, 2018
  - Sany/Ralls — Obama, 2012

- **Routine enquiries regarding un-notified transactions**

- **Mitigation compliance**
  - US$1 million fine for "repeated breaches"
Key Themes

Trend towards more scrutiny of investment around the world

- Driven by great power competition, economic integration and new vulnerabilities
  - Concerns over espionage, security of supply, technology transfer, technology leadership
  - Pre-dates Trump, driven by Congress and executive branch (not Trump) and will survive Trump
- Advanced countries enacting or reforming investment review procedures

Now a compliance obligation for companies taking investments, not just those making investments

- Focus on countries, companies and individuals presenting threats, but scrutiny across the market
- Legal and reputational risks
CFIUS Developments
European Union Export Control Developments
## European Union Export Control Developments

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Update on Proposed European Union Amendments to the Dual Use Controls</td>
</tr>
<tr>
<td>2</td>
<td>EU Recommendations and Requirements regarding Internal Control Programs</td>
</tr>
<tr>
<td>3</td>
<td>European Export Control Enforcement Update</td>
</tr>
<tr>
<td>4</td>
<td>Export Control and Economic Sanctions Implications of Brexit</td>
</tr>
<tr>
<td>5</td>
<td>European Foreign Investment Legislation</td>
</tr>
<tr>
<td>6</td>
<td>Export Control Implications of the European General Data Protection</td>
</tr>
</tbody>
</table>
Presenters

Ben Smith
Associate
London, United Kingdom
+44 20 7919 1088
ben.smith@bakermckenzie.com

Mattias Hedwall
Partner
Stockholm, Sweden
+46 8 56617733
mattias.hedwall@bakermckenzie.com

Helena Engfeldt
Associate
San Francisco, USA
+1 415 984 3842
helena.engfeldt@bakermckenzie.com
EU Dual-Use Regime
EU Dual-Use Regime

Recap

- EU Regulation 428/2009
  - Direct application in 28 (current) Member States
  - National licensing and enforcement (varying approaches)
- Exports of Annex I items to outside EU require export licence (Annex IV within EU)
- Intra-EU record-keeping and paperwork requirements
- "Exports" include physical and intangible transfers – broad application
- Key concept of "exporter"
- EU dual-use licences valid throughout the EU
- Brokering controls, limited to problematic end-uses (ML, WMD)
- No re-export or "deemed" export controls (in the US sense; though beware licence conditions)
- Compliance with export controls does not guarantee compliance with sanctions (or vice versa!) – i.e. also need to consider product controls, sectoral restrictions, designated parties, etc. from sanctions regimes
Updates to EU Dual-Use Control List


Amendments from Wassenaar Arrangement include:

- New entry for 'other' discrete microwave transistors (3A001b3f)
- New entry for signal generators with specified 'Radio Frequency modulation bandwidths' (3A002d5)
- New entry for software designed to restore operation of microcomputers/microprocessors after electromagnetic Pulse (EMP) or Electrostatic Discharge (ESD) disruption (3D005)
- New decontrol note for "Information security" items specially designed for a 'connected civil industry application' (5A002)
- Amendment to control entry for cryptographic activation token, including a Technical Note for the local definition of 'cryptographic activation token' (5A002)
- New entry for masks and reticles designed for optical sensors (6B002)
- Amendment to control entry for underwater submersible vehicles (8A001c)
- New entry for air-launch platforms for space launch vehicles (9A004g)
- Deletion of entry for technology for diffusion bonding for gas turbine engine components (9E003a7)
Proposals for 'Recast' Dual-Use Regulation

Where were we last year?

Commission proposals for amendment of 28 September 2016; aiming to modernise controls, increase controls on cyber-surveillance technologies, increase harmonisation and transparency, reduce burden on businesses

European Parliament agreed amendments on 17 January 2018

Proposals were with European Council (leaked papers suggest varying views across EU Member States, with strong resistance to certain key changes)

European Parliament and Council need to agree before legislation adopted

Proposals for 'Recast' Dual-Use Regulation

What has happened in 2019?

- Divergence between support in European Parliament (MEPs) and EU Council (Member States’ officials)
- Significant efforts within and between European Parliament and Council groups to try to find a proposal that could be agreed – but this wasn’t achieved before the end of the European Parliamentary term.
- In June 2019, ambassadors agreed the a negotiating position in the EU Council, where various proposals were rejected
- 21 October 2019 saw the first trilogue negotiation between the European Commission, European Parliament and Council as they seek to find a middle ground
Council position on key amendments

- Human rights end-use control

- Proposal for unilateral EU category 10 control list for cyber-surveillance items

- Potential new circumvention control

- Broad controls on "technical assistance" and "brokering" (including to impact subsidiaries/JVs of EU companies) through broadening of definitions

- New definitions of "export" and "exporter" to align with Union Customs Code, and requirement for guidance

- But - proposal to tie definition of "export" to a person rather than a destination (re cloud computing)

- Broadening available licences:
  - GEA for low value shipments (€5k or less)
  - GEAs for inter-company transmission of software and technology, encryption and large projects

- Focus on Internal Compliance Programmes – particularly for global export authorisations
EU Recommendations and Requirements regarding Internal Control Programs
EU Guidance on Internal Compliance Programme ("ICP")

Currently, no formal ICP requirement in the EU Regulation, but Art. 12(2) requires consideration of "proportionate and adequate means and procedures to ensure compliance" for global authorisations, and highly important step for exporters to minimise risks and operate efficiently and effectively.

In September 2018, Commission launched open public consultation on draft guidance for an effective ICP


Increasing importance of robust ICPs in light of proposals to update the Dual-Use Regulation

- Member States can request exporters using global export authorizations to implement an ICP
- Requirement for certain proposed EU GEAs
- Enforcement: knowledge and responses to compliance red flags (particularly for end-use controls)
EU Guidance on ICPs

Introducing the core elements

Key principles underpinning EU Guidance

Focus on risk assessments

Leveraging existing policies

Ensuring global compliance policies comply with EU law

7 core elements (non-exhaustive "cornerstones" for a company's tailored ICP):

- Top-level management commitment to compliance
- Organisation structure, responsibilities and resources
- Training and awareness raising
- Transaction screening process and procedures
- Performance review, audits, reporting and corrective actions
- Recordkeeping and documentation
- Physical and information security
5 Essential Elements of Compliance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Commitment</td>
<td>Commitment to Compliance</td>
<td>Management Commitment</td>
<td>Top level management commitment to compliance</td>
</tr>
<tr>
<td></td>
<td>Nomination of Responsible Personnel</td>
<td>Risk Assessment</td>
<td>Organisation structure, responsibilities and resources</td>
</tr>
<tr>
<td></td>
<td>Information and Training</td>
<td>Written EMCP</td>
<td>Training and awareness raising</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Company and Compliance Procedures</td>
<td>Compliance Training</td>
<td>Transaction screening process and procedures</td>
</tr>
<tr>
<td>Internal Controls</td>
<td>Suspicious Enquiries or Orders / End-Use Considerations</td>
<td>Adherence to Recordkeeping Regulatory Requirements</td>
<td>Performance review, audits, reporting and corrective actions</td>
</tr>
<tr>
<td>Testing and Auditing</td>
<td>Record Keeping</td>
<td>Compliance Monitoring and Periodic Audits/Assessments</td>
<td>Recordkeeping and documentation</td>
</tr>
<tr>
<td>Training</td>
<td>Provision for Audits</td>
<td>Internal Program for Handling Compliance Problems, including Reporting and Escalating Export Violations</td>
<td>Physical and information security</td>
</tr>
<tr>
<td></td>
<td>Integration with Quality Management Practices</td>
<td>Completing Appropriate Corrective Actions in Response to Export Violations</td>
<td></td>
</tr>
</tbody>
</table>
European Export Control Enforcement Update
UK – HMRC Annual Enforcement Report (25/05/2019)

- 278 consignments seized in last 2 years: military, dual-use, and goods subject to sanctions/embargoes.
- 265 potential exports prevented on end-use grounds i.e. because we had reason to suspect the goods might be used in a military or WMD programme.
- 55 Compound Penalties in lieu of prosecution since 2008 totaling almost £3 million.
- 27 prosecutions since 2005: exports, sanctions and trade controls.
## Recent UK Enforcement (public cases)

<table>
<thead>
<tr>
<th>Date made public</th>
<th>Violation</th>
<th>Type of penalty</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2019</td>
<td>UK trafficking and brokering controls</td>
<td>Compound penalty</td>
<td>£10,000 - £50,000</td>
</tr>
<tr>
<td>April 2019</td>
<td>Unlicensed Exports (Military)</td>
<td>Compound penalty</td>
<td>£50,000-£100,000</td>
</tr>
<tr>
<td>July 2018 – January 2019</td>
<td>Unlicensed Exports (Dual-Use)</td>
<td>Compound penalties (3 companies)</td>
<td>&lt;£10,000 x 3</td>
</tr>
<tr>
<td>November 2018</td>
<td>UK trafficking and brokering controls</td>
<td>Criminal prosecution</td>
<td>Prison sentences Plus recovery of profits (est. &gt;£5,000,000)</td>
</tr>
<tr>
<td>April 2018</td>
<td>Unlicensed Exports (Dual-Use and Military)</td>
<td>Criminal prosecution (guilty plea)</td>
<td>&lt;£10,000</td>
</tr>
<tr>
<td>April 2018</td>
<td>Unlicensed Exports (Military)</td>
<td>Compound penalty</td>
<td>&gt;£100,000</td>
</tr>
<tr>
<td>Date</td>
<td>Alleged Violation</td>
<td>Suspect</td>
<td>Penalty</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>13 November 2018</td>
<td>Unlicensed transit of military goods</td>
<td>Company</td>
<td>EUR 60,000 (30K)</td>
</tr>
<tr>
<td></td>
<td>(1 shipment, 9 products)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 February 2019</td>
<td>Unlicensed export of dual-use parts to Iran (catch-all)</td>
<td>Company (NL), Company (BAH),</td>
<td>EUR 500,000 (250K)</td>
</tr>
<tr>
<td></td>
<td>(Multiple shipments)</td>
<td>Shareholder, Director, Managing</td>
<td>EUR 350,000 (175K)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>employee, Former director</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>12 m prison (11) + 240 hrs service order</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8 m prison (7) + 200 hrs service order</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>180 hrs service order</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>120 hrs service order</td>
</tr>
<tr>
<td>20 February 2019</td>
<td>Export of sealing rings to Iran (EU sanctions)</td>
<td>Company</td>
<td>Acquittal</td>
</tr>
<tr>
<td></td>
<td>(2 shipments, 13 products)</td>
<td>Director</td>
<td></td>
</tr>
<tr>
<td>1 October 2019</td>
<td>Attempt to make goods available to DP (EU sanctions)</td>
<td>Company</td>
<td>EUR 5,000 (EUR 5K)</td>
</tr>
<tr>
<td></td>
<td>(1 shipment, 5 products)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Export Control and Economic Sanctions Implications of Brexit
Revised Withdrawal Agreement and Political Declaration agreed on 17 October 2019

- Declaration recognises sanctions as "a multilateral foreign policy tool and the benefits of close consultation and cooperation"

EU has granted a "flextension", delaying Brexit until 31 January 2020 unless the UK Parliament approves a deal beforehand in which case the UK will leave the EU on an earlier date

If a deal is approved, the UK will leave the EU and a transition period will run until 31 December 2020, unless extended by mutual agreement before 1 July 2020

- No change to current export controls or sanctions framework
- EU law, including the Common Foreign and Security Policy (CFSP), will continue to apply to the UK e.g., so the UK would have to implement EU sanctions introduced during transition (other than exceptional cases)
- But UK will no longer participate in EU institutions, including European Council and European Commission

In the event of a no deal or after a transition period, the European Union (Withdrawal) Act 2018 would broadly roll over EU law existing at that date and incorporate into UK law with UK Parliament deciding on changes over time
No Deal Brexit and UK Export Controls

Legal Framework
- EU (Withdrawal) Act 2018
- EU Dual-Use Regulation 428/2009
- Trade etc. in Dual-Use Items, Firearms and Torture etc. Goods (Amendment) (EU Exit) Regulations 2019
- Export Control (Amendment) (EU Exit) Regulations 2019
- International agreements (e.g. Wassenaar, MTCR, Australia Group and NSG)

Licensing
- UK regarded a third country vis-à-vis EU
- UK introduced EU OGEL
- EU added UK to UGEA 001
- EU export licences issued by the UK no longer valid for exports from the EU (and vice versa)
- UK to retain EU GEA in UK law (rGEA)

Policy
- Unlikely that UK will significantly relax export controls regime
- Unclear whether UK will mirror EU’s proposed changes to EU Dual-Use Regulation
- Limited impact on the UK’s military items and trafficking and brokering "trade controls" regimes
- Military and WMD-related end-use controls retained in the UK and would still apply in EU for exports to UK
# No Deal Brexit and UK Sanctions

## Legal Framework
- EU (Withdrawal) Act
- Sanctions and Anti-Money Laundering Act 2018 (SAML A)
- UK Statutory Instruments
- Review of EU DPs
- EU Blocking Regulation
- International organisations (e.g. UN and UNSC)

## Licensing
- UK more flexible in respect of sanctions licensing?
- UK licences will no longer cover exports/ provision of restricted services from the EU or activities of EU nationals (and vice versa)

## Policy
- UK to adopt and implement an autonomous sanctions regime – unlikely to shift significantly from EU
- However:
  - More aggressive approach regarding "owned or controlled"?
  - Broader approach in establishing UK jurisdiction?
  - More aggressive approach for Russia?
### What Should You Be Doing Now?

<table>
<thead>
<tr>
<th>UNDERSTAND</th>
<th>ACT</th>
<th>CONSIDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand supply chain (in full)</td>
<td>Understand export control classification of your products (e.g. Annex I items from UK to EU which wouldn't be controlled pre-Brexit, but post-Brexit would be)</td>
<td>Establishing exporting entities in the UK for exports from the UK, and in the EU for exports from the EU</td>
</tr>
<tr>
<td>Understand how your exports from UK to EU and vice versa will be affected by new licensing requirements</td>
<td>Understand impact of Brexit on sanctions and new sanctions regimes that will need to be considered for your shipments</td>
<td>Agreements with local subsidiaries</td>
</tr>
<tr>
<td>Monitor developments around the introduction of new UK sanctions regime</td>
<td>Understand impact of Brexit on existing export control licences</td>
<td>Local VAT registrations?</td>
</tr>
<tr>
<td></td>
<td>Check whether exports of controlled items are currently made from EU under a licence granted by the UK authorities, or from the UK under a licence granted by the EU authorities</td>
<td></td>
</tr>
<tr>
<td>Apply for new licences where needed, e.g.:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Register for EU OGEL on SPIRE for exports to EU;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Notify EU Member State of first use of UGEA 001 for exports to UK and check if pre-registration required; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Re-apply for new rGEA if current EU GEA is not registered on UK's licensing system</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

58
European Foreign Investment Legislation
EU – New Screening Framework

- New EU framework for screening FDI that raises security or public order concerns
- Review of FDI by EU Commission:
  - on the grounds of security and public order which affect projects of "Union interest"
  - projects involving substantial EU funding or in relation to critical infrastructure, critical technology or critical inputs
- No obligation on Member States to adopt national screening systems
- Member States may take into account if the foreign investor is state controlled, including through significant funding
- Easier to prohibit Chinese and other FDIs that fall short of acquisitions of control
UK – Current Status

Current Regime

- No foreign investment screening mechanism; under UK merger control rules, Government can intervene in deals raising "public interest" considerations in the UK (national security, plurality of the media, financial stability)
- Can also intervene in "special public interest" mergers — limited to defence and media
- Since 11 June 2018 – lower jurisdictional thresholds (£1m UK turnover of target and/or 25% UK share of supply) for military/dual-use, computing hardware and quantum technology sectors; voluntary notification

Recent Developments

- Proposals for standalone review of national security mergers
- Expanding voluntary regime to "call-in" transactions on national security grounds
- Potential application of rules to new projects, "proximate sites" and "bare asset" transactions
Export Control Implications of the European General Data Protection
GDPR – basics remain the same

Broad territorial scope, tension, legal bases

• Processing of personal data of EU residents by non-EU based company subject to the GDPR (Art. 3 GDPR)

• Justifying country/resident screenings and screenings against U.S. restricted or prohibited parties lists (Art. 6, 10 GDPR)

• Processing necessary for company's legitimate interests (Art. 6.1.f. GDPR)
September 2019 - Decision by the Swedish DPA

- Permission to screen against U.S. lists granted by Swedish DPA (limited to specific company)

- Relies on Swedish law supplementing Art. 10 GDPR and legitimate interest balancing under Art. 6.1.f.

- Permission conditioned on company otherwise complying with the GDPR

- Business friendly development, but limited to specific case/Sweden, contrast with Germany
GDPR – what should companies do?

DPIA, legal basis, strategic decisions, otherwise comply with the GDPR

- Complete a Data Protection Impact Assessment (Art. 35 GDPR)
- Decide on and document legal basis for processing (recent decisions from Swedish and Greek DPAs)
- Decide which group company should complete which screenings
European Union Export Control Developments
## Agenda

### Asia/Pacific Export Control Developments

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Japan: Removal of Korea from the &quot;White List&quot;</td>
</tr>
<tr>
<td>2</td>
<td>China: Proposed Export Control Regime</td>
</tr>
<tr>
<td>3</td>
<td>India: SCOMET Export Controls and Implications for the Information Technology Industry</td>
</tr>
</tbody>
</table>
## Asia-Pacific Export Control Overview

<table>
<thead>
<tr>
<th>Features</th>
<th>Australia</th>
<th>China</th>
<th>Hong Kong</th>
<th>Japan</th>
<th>Malaysia</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controlled items</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tangible</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intangible</td>
<td>Yes</td>
<td>Yes (Commercial Encryption)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Availability of classification ruling</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Controlled Activities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transit</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transshipment</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Import</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Brokerage</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deemed export</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Catch all (Use-based control)</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Penalties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fines</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Imprisonment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Asia-Pacific Export Control Overview

<table>
<thead>
<tr>
<th>Features</th>
<th>Singapore</th>
<th>Taiwan</th>
<th>Thailand</th>
<th>Indonesia</th>
<th>Philippines</th>
<th>Vietnam</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Controlled items</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tangible</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intangible</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Availability of classification</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ruling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Controlled Activities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (limited goods)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transit</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Transshipment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Import</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Brokerage</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deemed export</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Catch all (Use-based control)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Penalties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Imprisonment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Japan: Removal of Korea from the "White List"
1. Bulk license applicability: individual export licenses now required for certain items and related technologies

METI (Ministry of Economy, Trade and Industry) announced partial amendments to four guidelines related to the implementation of export control regulations, including the Export Trade Control Order.

Starting on July 4, 2019, Japanese exporters have been required to apply for individual export licenses to export the following materials to the Republic of Korea:

- Hydrogen Fluoride;
- Fluorinated polyimide;
- Resist;

and their relevant technologies, which may be related with semiconductors manufacturing technologies.

Bulk licenses for these three materials are no longer available.
1. Bulk license applicability: individual export licenses now required for certain items and related technologies

The office responsible for receiving export license applications for exports of these materials to the Republic of Korea has been changed:

from METI bureau or branch office

to the Security Export Licensing Division of METI's main office.
2. Removal of Korea from the "White List"

METI amended the Export Trade Control Order removing the Republic of Korea from the "White Countries" list. This went into effective on August 28, 2019.
3. Rationale and Implications

National Security Reason

The rationale for these measures by Japanese government is:

Since the government realized that certain controlled products were transferred to sanctioned countries after they were exported to the Republic of Korea, they need to scrutinize exports of specific items to the Republic of Korea.

Japanese government considered that the Republic of Korea is no longer qualified for "White Countries".
3. Impact on the market

(1) Bulk License Applicability

Bulk license is very convenient. Once it is obtained, it is valid for certain period of time, e.g. three years, and it can be extended.

Application for an individual license at each time of each shipment is time consuming.

This amendment had an impact on the global semiconductor supply chain, as semiconductors are manufactured from various materials and parts obtained from interconnected suppliers.

Individual licenses have been issued by Japanese government since then.
3. Impact on the market

(2) Removal from "White Countries" list

Exports to "White Countries" are subject to simpler export licensing requirements and rarely require an export license unless they involve the export or transfer of so-called "listed products / technologies".

If the destination is a non-White Country, an export license is sometimes required even when the products /technologies at issue are not "listed products / technologies".

Exports from Japan to the Republic of Korea are subject to scrutiny of end user and end use.
3. Impact on the market

(3) Scrutiny

In these days, export license application process has become more strict than before not only on export to South Korea but also export to other non-White Countries.

For example, end use certificates issued by end customers of finished products are required for certain products.

We see certain change of policy in implementation practice of export control regulations.
3. Impact on the market

(3) Time consuming

Due to these amendments and change in practice, there are more export license applications than it used to be, which takes applicants longer time to obtain an export license.
3. Impact on the market

(4) Technology Transfer Control Requirement v. Smooth transfer of goods/Technologies (Free Trade)

It has been concerned that the export control of the technology transfer in Japan was not sufficient and that it should be strict as that in US, EU or China.

The authority is trying to find the best solution between technology transfer control and free trade.
3. Impact on the market

(5) Dispute under WTO
These measures are now disputed under WTO (DS590).
The Republic Korea filed the case based on the violation of:
Article I of the GATT 1994 (most favored nation's treatment)
Article XI:1 of the GATT 1994 (export restriction)
China: Proposed Export Controls Regime
## Chinese export control law – would the trade war impact the implementation timeline?

<table>
<thead>
<tr>
<th>Draft export control law issued by MOFCOM in 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed to have extra-territorial application similar to the US export control law</td>
</tr>
<tr>
<td>Initially expected to be finalized early next year. <strong>Will the finalization of the law be expedited in view of the trade war?</strong></td>
</tr>
</tbody>
</table>
### Chinese export control law key concepts

<table>
<thead>
<tr>
<th>Controlled items</th>
<th>Deemed export</th>
<th>Re-export</th>
<th>Licensing requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>The controlled items include dual-use items, military products, nuclear materials and others that have implications for national security – include tangible goods, technologies and services</td>
<td>Include &quot;deemed export&quot; concept which can apply to in-country transfer to non-Chinese persons</td>
<td>Include &quot;re-export&quot; concept which can apply to transfer between two non-Chinese jurisdictions, based on the origin of goods/technology</td>
<td>Allows for licensing authorities to issue &quot;general licenses&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Listing mechanism</th>
<th>Black-listing control</th>
<th>Internal compliance program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government may list goods/technologies as controlled items in times of war or in &quot;urgent situations&quot;, and take provisional measures</td>
<td>Provides black-listed control that includes foreign importers and end-users who fail to fulfil end-user / end-use commitments, who may pose threats to national security or use the items for terrorist purposes</td>
<td>Encourages enterprises to establish internal compliance program (&quot;ICP&quot;) for export control, and may grant licensing facilitations to enterprises which adopt ICP</td>
</tr>
</tbody>
</table>
Chinese reaction to the US measures: Unreliable entity list

What does it mean if your company / customer falls within the list?

**Background**
- Announced by MOFCOM on 31 May 2019
- Black-listing foreign entities / individuals that boycott / cut off supplies to Chinese companies
- Inform the public of risks involved in dealing with the listed entities

**Procedure and standard**
- To be stipulated in new regulations, to cover:
  - Investigation
  - Interested parties’ right to argue their cases
  - Removal from the list where remedial actions are taken

**Blacklisting considerations**
- Discriminatory measures against Chinese companies
- Whether for non-commercial purposes and against market rules / contractual obligations
- Material damage to Chinese companies
- Potential threat to China’s national security

**Potential actions**
- To be determined under framework of existing laws and regulations, e.g.:
  - Refusal of transaction
  - Imposition of discriminatory conditions or prices
  - Launch of a “national security review” mechanism

Can a person be subject to conflicting obligations under the US / China laws?
India: SCOMET Export Controls and Implications for the Information Technology Industry
India's Implementation of the Wassenaar Dual Use Export Control List

- SCOMET Article 8
- Specifically includes software and technology
  - Encryption software is classified under SCOMET Category 8D502 (the equivalent of ECCN 5D002)
Establishes an export license called the General Authorization for Intra-Company Transfers (GAICT) for SCOMET Items/Software/Technology

- The GAICT authorizes "re-exports" of SCOMET controlled items, including software and technology by an Indian subsidiary to a foreign parent corporation or to other subsidiaries of that foreign parent corporation

- The CAICT does not authorize such "re-exports" from Indian third party contractors to foreign principals in a contract development relationship

- The CAICT does not authorize such "re-exports" from an Indian parent corporation to its foreign subsidiary
Conditions on Eligibility and Use of the GAICT

- There must be a Master Services Agreement between the foreign parent corporation and the Indian subsidiary
- The software or technology must have been originally exported by the foreign parent corporation to the Indian subsidiary under a "License Exception"
  - Does this include a general license such as the UK OGEL for cryptographic development?
- The Indian subsidiary may not change the "functionality" of the software or technology
  - What are the implications for a research and development project between the foreign parent corporation and the Indian subsidiary
The Indian subsidiary must have an approved ICP, or must demonstrate its compliance with the parent corporation's ICP.

The Indian subsidiary must agree to on-site inspections to verify compliance.

Subsequent re-exports of software or technology re-exported from Indian under the GAICT must be made in conformance with the export control laws and regulations of the foreign parent corporation.

Quarterly reports of exports made under authority of the GAICT are required.

- Each quarterly report must include end-user certificates (query, whether the end-use certificate must be furnished only by the parent corporation or by downstream customers?)
What is required in the quarterly reports where the Indian subsidiary and the foreign parent exchange software code or technology on a daily basis in furtherance of a development project?
Other Jurisdictions
Proposed abolition of the death penalty

- The Malaysian government rowed back on earlier plans to abolish death penalty and announced in March 2019 that it will only abolish mandatory capital punishment and will leave it to courts to decide whether death penalty is appropriate punishment for serious offences.

- The Strategic Trade Act 2010 ("STA") provides for possible death penalty for offences committed with intent involving arms or related material resulting in death.

Regulations on compounding of offences

- Earlier amendments to the STA in 2017 include the introduction of the power for the Ministry of International Trade and Industry ("MITI") to compound offences under the STA.

- MITI issued a public consultation paper to invite public feedback on the issuance of regulations on the compounding of offences in late October 2019.

- Minimum compound of 3% of the maximum fine for the relevant offence is suggested.
Thailand

Trade Control on Weapons of Mass Destruction Related Items Act ("WMD Act") passed

• On 30 April 2019, the WMD Act was enacted and announced in the Royal Gazette, and its main provisions will become effective on 1 January 2020.

• Controlled items under the WMD Act include WMDs, armaments and dual-use items ("DUI") as well as tangible and intangible items that could have commercial interest, technology or even software. It is expected the Ministry of Commerce will subsequently issue its DUI list, based on the latest EU Dual-Use Item List.

• Controlled activities include export, re-export, transshipment, transit, brokerage and other actions with the purpose of spreading WMDs.

• Upon coming into force of the WMD Act, the Ministerial Notification Regulating the Dual-Use Items dated 16 October 2015 is expected to be cancelled.
Implementation of the Strategic Trade Management Act further delayed

- Although the law has been in place since 2015, its implementation has been deferred several times.
- At this time, it is difficult to determine when the Philippine government will actually implement the same.

### Phased Implementation Timeline

<table>
<thead>
<tr>
<th>Service</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>January 2019</td>
</tr>
<tr>
<td>Export</td>
<td>June 2019</td>
</tr>
<tr>
<td>Transit/Transhipment</td>
<td>January 2020</td>
</tr>
<tr>
<td>Re-export/Reassignment</td>
<td>June 2020</td>
</tr>
<tr>
<td>Related Services</td>
<td>January 2021</td>
</tr>
<tr>
<td>Import</td>
<td>June 2021</td>
</tr>
</tbody>
</table>
Singapore

Process and controlled-category changes

- Voluntary disclosure process moved to online submission
- Changes to list of controlled items in transit or for transhipment that are exempt from needing a permit
- Changes to controlled items under brokering regulations
- Other form and process changes - so check your screening and processes are up to date
Expected changes to intangible transfers regime

• Review of Defence Trade Controls Act 2012 tabled in Parliament in February 2019
• Government supported the proposed changes - most recommendations about improving administration of laws
• Unlikely inter-company transfers will become exempt from permit
Asia / Pacific Export Control Developments
Canada Export Control Developments
Agenda

Canada Export Control Developments

1 Export Control Developments

2 Sanctions Developments
Export Control Developments
Order Amending the Export Control List (ECL)

In force as of May 17, 2019

<table>
<thead>
<tr>
<th>Export Control Regime</th>
<th>Latest Controls Incorporated into ECL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wassenaar Arrangement</td>
<td>December 2016</td>
</tr>
<tr>
<td>Nuclear Suppliers Group</td>
<td>June 2016</td>
</tr>
<tr>
<td>Missile Technology Control Regime</td>
<td>October 2016</td>
</tr>
<tr>
<td>Australia Group</td>
<td>June 2016</td>
</tr>
</tbody>
</table>

- December 2016 version of the "A Guide To Canada's Export Control List" (Guide)
Amendments to the Export and Import Permits Act (EIPA)

In force as of September 1, 2019 (Bill C-47)

• As part of Canada's support for a stronger and more rigorous export control system, the Government of Canada committed to joining the Arms Trade Treaty (ATT)

• The legislative and regulatory changes giving effect to Canada's ascension to the ATT came into force on September 1, 2019

• Canada became a State Party to the ATT on September 17, 2019

• Global Affairs Canada (GAC) "Arms Trade Treaty Regulatory Implementation Package" website
Amendments to the EIPA (cont'd.)

In force as of September 1, 2019 (Bill C-47)

Bill C-47 amended the EIPA to establish controls over brokering by:

1. defining brokering
2. amending the *Criminal Code* to make brokering without a permit a criminal offence, and
3. giving the Government of Canada the authority to establish a Brokering Control List, Brokering Permit Regulations, and other regulations related to brokering
Amendments to the EIPA (cont'd.)

Amendments and new regulations

- ECL amended to include a new Group 9 (ATT)
  - Amendments in the regulation, not in the December 2016 Guide
- **Brokering Control List**: Includes all Munitions List (Group 2) and Arms Trade Treaty (Group 9) items, and may include any article on the ECL that, at the determination of the Governor-in-Council, is likely to be used to produce or develop a weapon of mass destruction. The specific descriptions and conditions attached to each article, however, may differ from those found for the associated article in the ECL
  - chemical/biological weapons; nuclear explosive or radiological dispersal devices; related material or equipment for use in such weapons; missile or delivery systems for such weapons, or related material or equipment for use in such missile or delivery systems
  - Groups 1, 3, 4, 6 and 7 and sub items 5504(2)(d), (e) and (g)
Amendments and new regulations

- **Brokering Permit Regulations**: Sets out the information that an applicant must submit in their application for an individual brokering permit (e.g., information about the seller, buyer and any other agents or brokers involved; and information on the goods to be brokered, including on their proposed end use)

- **Regulations Specifying Activities that Do Not Constitute Brokering**: specifies activities that, while technically falling under the EIPA's definition of "brokering," will be excluded from the new controls (e.g., transfers between affiliates of a corporation)
Amendments and new regulations

• **General Brokering Permit (GBP) No. 1**: This regulation creates a General Permit that can be used to broker in pre-defined, lower-risk circumstances. This GBP authorizes brokering to certain low-risk destinations, provided that the end use is in that destination and that the broker follows the requirements set out in the GBP
  • Can be used by "any person or organization"

• **General Export Permit (GEP) No. 47** – The objective of GEP 47 is to provide a streamlined permitting process for the export of most ATT items to the United States
  • Can be used by "a resident of Canada"
Amendments to the EIPA (cont’d.)

Mandatory human rights considerations

• The Minister shall take into consideration whether the goods or technology specified in the application for the permit (export permit or brokering permit) (a) would contribute to peace and security or undermine it; and (b) could be used to commit or facilitate
  (i) a serious violation of international humanitarian law,
  (ii) a serious violation of international human rights law,
  (iii) an act constituting an offence under international conventions or protocols relating to terrorism to which Canada is a party,
  (iv) an act constituting an offence under international conventions or protocols relating to transnational organized crime to which Canada is a party, or
  (v) serious acts of gender-based violence or serious acts of violence against women and children
Amendments to the EIPA (cont'd.)

Mandatory human rights considerations

• "Substantial risk" test
  • applied to export and brokering permits for strategic goods and technology included in the ECL and in the Brokering Control List in respect of arms, ammunition, implements or munitions of war or having an end-use related to weapons of mass destruction
  • should be a connection, based on compelling evidence, between the negative consequences and the specific goods or technology proposed for export or brokering
  • Various factors/considerations could be taken into account
Amendments to the EIPA (cont'd.)

Offences and Penalties

- Maximum fine for summary conviction increased from CAD $25,000 to $250,000
- The amended EIPA prohibits unauthorized brokering by any legal or natural person or organization in Canada. Canada's brokering controls also apply abroad to:
  - Canadian citizens,
  - Permanent residents, or
  - Organizations as defined in section 2 of the *Criminal Code* that are incorporated, formed or otherwise organized under the laws of Canada or a province
Other Notable Export Control Developments

• CBSA continues to develop its export audit program
  • If you have an export voluntary disclosure outstanding with the CBSA, be proactive and follow-up to close out the file
• Export Controls Online (EXCOL) is in the process of being upgraded
  • Maintain your EXCOL account information – EXCOL registrants are responsible for advising GAC of any changes to the company officials or recognized users identified/authorized under EXCOL
Sanctions Developments
2019 Sanctions Developments

Quick Summary

• "Housekeeping" amendments:
  • Regulations Amending Certain Regulations Made Under the United Nations Act (SOR/2019-60)
  • Regulations Amending Certain Regulations Made Under the Special Economic Measures Act (SOR/2019-61)
• Amendments to designated/listed persons
  • Russia (March 14); Ukraine (March 4, March 15, June 25)
  • Venezuela (March 4, April 15, June 25)
• Enactment of new sanctions
  • Nicaragua (June 21)
• Order extending the sanctions against Ukraine under the Freezing Assets of Corrupt Foreign Officials Act for an additional 5-year period beginning on March 6, 2019
Lists of Designated/Listed Persons

• Office of the Superintendent of Financial Institutions (OSFI) no longer maintaining a list of individuals/entities under the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism, United Nations Al-Qaida and Taliban Regulations, and Criminal Code
  • UN sanctions → UN Al-Qaida and Taliban Sanctions Lists
  • Criminal Code → Public Safety Canada's "Currently listed entities" page (but note the disclaimer)

• The Canadian Autonomous Sanctions List (GAC)
  (i) disclaimer → "administrative purposes only"
  (ii) only includes names from the Special Economic Measures Act and the Justice for Victims of Corrupt Foreign Officials Act
    • Missing: UN Sanctions, Criminal Code, Freezing Assets of Corrupt Foreign Officials Act
Canada Export Control Developments
Economic Sanctions
## Agenda

### United States Economic Sanctions Programs

<table>
<thead>
<tr>
<th></th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Iran</td>
</tr>
<tr>
<td>2</td>
<td>Russia</td>
</tr>
<tr>
<td>3</td>
<td>Venezuela</td>
</tr>
<tr>
<td>4</td>
<td>Cuba</td>
</tr>
<tr>
<td>5</td>
<td>Turkey</td>
</tr>
<tr>
<td>6</td>
<td>OFAC Updates to Part 501 in June 2019</td>
</tr>
</tbody>
</table>
Iran
US Sanctions Targeting Iran

Secondary Sanctions

Significant Reduction Exceptions not renewed after May 2, 2019

- "Our firm policy is to completely zero out purchases of Iranian oil – period. Any new purchases of oil initiated after the expiration of the SREs on May 2 will be subject to US sanctions, even if a country had not met its previously negotiated purchase caps during the SRE period from November to May 2." Brian Hook, US Special Rep. for Iran, May 30, 2019

Executive Order 13871 (May 8, 2019) – targets iron, steel, aluminum, and copper sectors

Findings under Section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012 October 31, 2019

- Construction sector controlled by the IRGC: sale, supply, or transfer to or from Iran of raw and semi-finished metals, graphite, coal, and software for integrating industrial purposes will be sanctionable if those materials are to be used in connection with the Iranian construction sector
- Four strategic materials are used in connection with the nuclear, military, or ballistic missile programs and will be sanctionable regardless of end-use/end-user
## US Sanctions Targeting Iran

### High-Profile Designations

<table>
<thead>
<tr>
<th>Designation of the IRGC as a Foreign Terrorist Organization (April 8, 2019)</th>
<th>Designation of Iranian Foreign Minister Javad Zarif (July 31, 2019)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Order 13876 (June 24, 2019) – Designates the Supreme Leader of Iran (currently, Ayatollah Khamenei) and others as SDNs; authorizes further designations</td>
<td>Designation of the National Development Fund and Etemad Tejarat Pars Co.; additional Specially Designated Global Terrorist sanctions on Central Bank of Iran (Sept. 20, 2019)</td>
</tr>
<tr>
<td>Designation of seven entities in Iran's global nuclear procurement network (July 18, 2019)</td>
<td>Subsidiaries of Chinese shipping company (September 25, 2019)</td>
</tr>
</tbody>
</table>
The Problem of the EU Iran Blocking Regulation

Conflict between EU and US laws

- EU persons in the US; US persons in the EU
- US owned/controlled entities incorporated in EU
- Application of US sanctions to EU persons/entities outside EU
- Risks: regulatory and litigation risk (recent cases in the UK, NL, Germany, Italy)

Navigating a path

- EU parties complying with US sanctions? Prohibited
- EU parties making commercial/financial decisions? Permitted
- EU parties complying with EU sanctions/other laws (ABC, AML etc)? Permitted
- EU parties deferring decisions to US parent, complying with global policies? Mitigates risk
- Case by case arguments as to why the EU Blocking Regulation does not bite
UN/EU sanctions – risk of snapback

- While EU remains committed to JCPOA, recent EU/UK threats to invoke UN JCPOA dispute resolution procedure in event of further Iranian breach
- Could result in UN snapback
- In which case, EU has said it will bring all former sanctions back into force (albeit needs unanimity)
- Includes:
  - Extensive DP controls (including most banks)
  - Funds transfer controls
  - Extensive controls on the banking, insurance, shipping, oil and gas, construction and other sectors
US Sanctions Targeting Russia

SDN-Related Developments
- Delisting of En+ Group, Rusal, EuroSibEnergo (January 27, 2019)
- Extension through Mar. 31, 2020 of two general licenses authorizing certain transactions involving GAZ Group (Nov. 1 2019)
- SDN designations for attacks on Ukrainian naval vessels in Kerch Straight, interference in 2018 midterm elections, sanctions evasion

CBW Act Sanctions
- Imposed by US State Department under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 ("CBW Act") in response to the poisoning of former Russian spy and his daughter in the UK
- The first round targeted exports of certain goods and technology to Russia, but included numerous waivers
- The second round was implemented August 2019; no real effect unless exporting CB items

Secondary Sanctions
- Introduced in Countering America's Adversaries Through Sanctions Act ("CAATSA") in August 2017
- Secondary (i.e., extraterritorial) sanctions on parties (US and/or non-US, depending on the provision) who engage in activities that include: investments in "special Russian crude oil projects"; sanctions on parties engaging in significant transactions with the Russian intelligence or defense sectors; sanctions related to Russian energy export pipelines; sanctions related to investments in the privatization of Russia's state-owned assets.
Russia: New EU Sanctions Regimes

**October 2018**

New EU chemical weapons sanctions regime (introduced in response to use of chemical weapons in Syria, and to the poisoning of Sergei and Yulia Skripal)

- Designated Party controls applying to persons involved in chemical weapons-related activities
- 9 individuals and 1 entity designated to date

**May 2019**

New EU cyber-attacks sanctions regime (introduced in response to fears around election integrity)

- Designated Party controls applying to persons involved in cyber-attacks targeting the EU or Member States
- No designations to date
Russian Responses to Western Sanctions

Overview and recent developments

**Travel ban** for certain western politicians (list is not fully disclosed)

**Food import ban**: covers US/EU and other jurisdictions implementing sanctions against Russia

**Recent Developments:**

- Law on Russian Countermeasures
  - *Six potential countermeasures* against "unfriendly foreign states" and legal entities thereof: suspension of international cooperation; import/export restrictions; public procurement restrictions; restrictions on the privatization of state and municipal property; other measured determined by the President
  - The suggested restrictive countermeasures **have not been imposed against any US/EU companies so far**
- New corporate data disclosure regulations (cases are established when Russian companies are allowed not to disclose their shareholders/managers referring to sanctions)
- New Russian countersanctions against **Ukraine** (blocked persons; export/import restrictions)
Russian Responses to Western Sanctions

New corporate data disclosure regulations

• On April 4, 2019 the Russian Government issued Decree No. 400 allowing securities issuers (joint stock companies) not to disclose information (shareholding and management information; information on affiliated persons and subsidiaries, etc.) if the issuer is a sanctioned person or if such disclosure of information about a sanctioned person would (or is likely) to result in the imposition of sanctions against the issuer, or any third parties, or the sanctioned person

• On August 15, 2019 the Russian President issued Decree No. 388, establishing a special record-keeping regime:
  • the registrar shall provide information on shareholders, excluding the information on sanctioned Russian shareholders
  • this rule applies if the issuer has notified the registrar about such sanctioned shareholders

• On September 7, 2019 the Russian Government issued Decree No. 1173 allowing Russian credit institutions to not fully disclose information normally subject to mandatory disclosure (shareholding and management information; information on affiliated persons and subsidiaries, etc.) if such disclosure would (or is likely) to result in the imposition of sanctions against the credit institution, or any third parties; or if the credit institution is a sanctioned person
Russian Responses to Western Sanctions

Sanctions against Ukraine

Since October 22, 2018, Russia has been implementing sanctions against Ukraine. These sanctions have been applicable to:

- 567 individuals and 75 entities specifically named on the sanctions lists
- Any entities controlled by such listed persons

The restrictive measures require Russian persons:

- To block non-cash funds, non-documentary securities and property of sanctioned Ukrainian persons located in Russia
- To refrain from participating in financial transactions with such sanctioned persons (Russian financial institutions will freeze such financial transactions)

Since December 29, 2018, Russia applies certain export/import restrictions against Ukraine
## Russian Responses to Western Sanctions

### Sanctions draft bills (1)

<table>
<thead>
<tr>
<th>No.</th>
<th>Proposed measure</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>464757-7</td>
<td>Criminal liability for (i) complying with sanctions imposed by the US/EU/other states and (ii) contributing to the implementation of sanctions against Russia</td>
<td>Consideration was suspended in May 2018 due to a strong criticism from the Russian business community. The Draft bill is unlikely to ever be adopted</td>
</tr>
<tr>
<td>754380-7</td>
<td>(i) to subject the disputes between sanctioned Russian persons and their foreign counterparties to the jurisdiction of courts/arbitral tribunals located in Russia; (ii) to grant Russian persons the right to unilaterally amend arbitration provisions providing for the settlement of disputes in states other than Russia, so that the cases can be settled by courts/arbitral tribunals located in Russia</td>
<td>Approved by the Russian State Duma in the 1st reading on July 24, 2019 (no further actions to date)</td>
</tr>
</tbody>
</table>
# Russian Responses to Western Sanctions

## Sanctions draft bills (2)

<table>
<thead>
<tr>
<th>No.</th>
<th>Proposed measure</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>710110-7</td>
<td>To ban the collection, transfer and public distribution of (i) information contributing to the imposition of sanctions against Russia; (ii) information showing that particular sanctioned Russian persons failed to observe the sanctions imposed</td>
<td>On October 28, 2019 the State Duma proposed to withdraw the Draft bill (i.e., it is likely that the Bill will not be adopted)</td>
</tr>
<tr>
<td>710099-7</td>
<td>To impose criminal liability for certain actions with the above-mentioned information, such as (i) public distribution or (ii) collection, transfer, stealing or storage aimed at public distribution or transfer to entities of unfriendly states</td>
<td>Was strongly criticized by the Russian Government and was found to be contrary to the Russian Constitution by the State Duma on October 24, 2019 (i.e., the Bill will not be adopted)</td>
</tr>
</tbody>
</table>
Screening Potential Business Partners in Russia

Best practices (1)

• Screening tools:
  • Russian State Register of Legal Entities (a.k.a. EGRUL) – contains ownership and management information of Russian LLCs (egrul.nalog.ru)
  • Spark database – the most comprehensive search tool, provides information available in the EGRUL, as well as other publicly disclosed data (www.spark-interfax.ru)
  • Corporate documents that Russian PJSCs must disclose (lists of affiliates; quarterly and annual reports, etc.) – contain ownership and management information of Russian PJSCs
  • Corporate websites (both of the target and of its affiliates)
  • Open sources (mass media publications)
  • In all unclear cases request your Russian counterparty to disclose its ownership and management information in writing
Screening Potential Business Partners in Russia

Best practices (2)

- Key aspects for consideration:
  - **No-penalty** approach to sanctions screening in Russia
  - Ownership and managements structures are often not transparent (JSCs are not required to disclose their ownership/management structure + new corporate data disclosure regulations)
  - Transactions with complex structures should be analyzed very carefully
  - **No-penalty** approach to trade compliance clauses in Russia
  - Sanctions compliance clauses may or may not work in Russian courts (Russian authorities do not recognize the legitimacy of sanctions imposed against Russia), but practice shows that Russian business partners are usually willing to cooperate with their foreign counterparties and respect sanctions compliance provisions in contracts
  - **Practice**: need to carefully screen and use trade compliance clauses in the entire CIS !!!
Venezuela
# US Sanctions Targeting Venezuela

**January 8, 2019** – SDN designations of 30 persons over a corruption scheme concerning the Venezuelan Government's currency exchange practices

**January 28, 2019** – PDVSA designated as SDN

**Various other SDN designations**

- Central Bank of Venezuela
- Evrofinance Mosnarbank (Russian bank)
- CVG Compania General de Mineria de Venezuela CA (MINERVEN) (Venezuelan state-owned gold mining company)
- Banco de Desarrollo Economico y Social de Venezuela (BANDES) and four financial institutions it owns or controls (limited general licenses)
- Banco Central de Venezuela (Venezuela's central bank)
- Cubametales (Cuban state-owned oil company; importation of oil from Venezuela)
- Vessels and companies involved in Venezuelan oil trade
- Parties connected to Maduro regime
US Sanctions Targeting Venezuela

May 24, 2019 – EAR: Venezuela moved to Country Groups D:1, D:2, D:3, D:4 – countries of national security, nuclear, chemical and biological weapons, and missile technology concerns

August 5, 2019 – Executive Order blocking the Government of Venezuela (including owned or controlled entities)

- Various general licenses, including:
  - GL 28 – wind-down (expired 4 September)
  - GL 27 – intellectual property
  - GL 30 – operations or use of ports and airports
  - GL 31 – transactions with interim government of Juan Guaidó
  - GL 34 (issued September 9) – certain GOV-related individuals

SDN removals – Christopher Figuera (May 7), PB Tankers (July 3), other shipping companies/vessels (September 24)
Cuba
US Sanctions Targeting Cuba

April 17 – US would end suspension of Title III of Helms-Burton Act

June 4 – restricting group people-to-people educational travel; limiting types of aircraft/vessels authorized to travel to Cuba on temporary sojourn

Sept. 6 – eliminates U-turn financial transactions; restricts remittances

Oct. 21 – re-sets de minimis to 10%; adds restrictions to License Exceptions AVS and SCP; general policy of denial for leases of aircraft to Cuban state-owned airlines

Oct. 24 – US to suspend flights between the United States and Cuban cities other than Havana in the next 45 days

Note: EU Blocking Regulation applies re US Cuba sanctions (as well as re US Iran sanctions)
Turkey
US Sanctions Targeting Turkey

Executive Order 13894 (Oct. 14, 2019)

- Broad blocking authorities includes:
  - parties involved in destabilizing activities in Syria or human rights abuses
  - GOT current or former officials, agencies, etc.
  - parties who operate in sectors of the Turkish economy (TBD)
  - parties who assist, support, etc., SDNs designated under the EO
  - parties owned or controlled by or who have acted on behalf of SDNs

- Secondary sanctions risks
  - non-US persons involved in military/political activities in northern Syria
  - foreign financial institutions who have knowingly facilitated significant financial transactions for SDNs
  - SDN included 3 Turkish ministers, Ministry of Energy and Natural Resources, Ministry of National Defense but REMOVED on 23 Oct.

Indictment against Halkbank (October 15, 2019)

Possible CAATSA sanctions for purchase of S-400 from Russia
OFAC Updates to Part 501 in June 2019
OFAC Updates to Part 501 in June 2019
Clarification or Expansion of Reporting Requirements?

- "Blocked"/frozen property still needs to be reported within 10 business days
- Blocked property reporting forms revamped for financial/non-financial transactions
- Unblocking property reporting requirements at 31 CFR § 501.603(a)(3)
- Changes to "rejected transactions" reporting requirements at 31 CFR § 501.604

- Previously limited to financial institutions, but amended to cover US Persons and persons subject to US jurisdiction
- Include wire transfers, trade finance, securities, checks, foreign exchange, and goods or services
- OFAC rejected-transactions reporting form still focused on financial transactions
- Not clear what constitutes a "rejected transaction" outside of banking sector
- Uncertainty about application of this reporting requirement among OFAC bar
Economic Sanctions
COFFEE BREAK
Export Control and Economic Sanctions Enforcement Developments
Agenda

Export Control and Economic Sanctions Enforcement Developments

1. Summary of 2019 Enforcement Activity
2. Selected Enforcement Matters
3. OFAC Enforcement Guidelines and Compliance Framework
4. DOJ Guidance on Evaluation of Corporate Compliance Programs
5. Cross-Border Investigations Issues
Summary of 2019 Enforcement Activity
OFAC 2019 Enforcement Activity

- To date in 2019, OFAC has settled **twenty-two** enforcement actions with an aggregate settlement value of **USD 1,288,112,800**
- 2018: 7 cases with an aggregate value of almost USD 72 million
  - 2017: 16 cases with an aggregate value of almost USD 120 million
  - 2016: 9 cases with an aggregate value of almost USD 22 million
  - 2015: 15 cases with an aggregate value of almost USD 600 million
- Significant cases involved the following companies:
  - The General Electric Company
  - British Arab Commercial Bank plc
  - UniCredit Bank
  - Standard Chartered Bank
OEE 2019 Enforcement Activity

- To date in 2019, OEE has brought twenty-four enforcement actions, which were primarily against individuals.
- Mahan Airways is the most high-profile case. According to OEE, the case was based on evidence developed during the investigation that indicated a "blatant disregard of U.S. export controls" and existing TDO.
- 2018: 42 cases
- 2017: 54 cases
- 2016: 41 cases
- 2015: 41 cases
2

Selected Enforcement Matters
Selected OFAC Enforcement Matters

- Standard Chartered Bank
- UniCredit Bank
- British Arab Commercial Bank plc
- KollMorgen
- Haverly Systems
- e.l.f. Cosmetics
- Cuba travel cases
Selected Secondary Sanctions Actions

- Evrofinance Mosnarbank
- PB Tankers
- Dalian units of China COSCO Shipping Corp.
- Case comparison: Turkey's S-400 air defense system purchase from Russia versus China's purchase from Russia of 10 SU-35 combat aircraft in 2017 and S-400 surface-to-air missile system-related equipment in 2018
Selected Criminal Actions

- Huawei
- Halkbank
- China General Nuclear Power Group
3

OFAC Enforcement Guidelines and Compliance Framework
OFAC Enforcement Guidelines

**General Factors:**
- Willfull or reckless violation of law
- Awareness of conduct at issue (including knowledge of senior management)
- Harm to sanctions program objectives
- Individual characteristics (e.g., commercial sophistication, volume of transactions)
- Compliance program
- Remedial response
- Cooperation with OFAC
- Timing of apparent violation in relation to imposition of sanctions
- Other enforcement action by gov’t agencies
- Future compliance/deterrence effect
- Other relevant factors on case-by-case basis

**Base Penalty Matrix**

<table>
<thead>
<tr>
<th>Voluntary Self-Disclosure</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Egregious Case</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One-Half Transaction Value (capped at lesser of $151,292 or one-half of the applicable statutory maximum per violation)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Applicable Schedule Maximum</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One-Half of Applicable Schedule Maximum</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applicable Statutory Maximum</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
OFAC Compliance Framework

Published May 2, 2019

- Essential components of a sanctions compliance program
  - Management Commitment
  - Risk Assessment
  - Internal Controls
  - Testing and Auditing
  - Training

- OFAC will consider whether a company had an effective sanctions compliance program in determining whether a violation was "egregious"

- OFAC may incorporate these components into settlement agreements
DOJ Guidance on Evaluation of Corporate Compliance Programs
Background to DOJ's evaluation guidance

- Original version of the DOJ's Guidance on Evaluation of Corporate Compliance Programs issued in February 2017
- At that time, DOJ had a dedicated position of "compliance counsel" within the Department as an experienced compliance expert who was to advise prosecutors on corporate compliance and to assess companies' compliance programs during the corporate criminal resolution process
- The original Guidance included a set of questions that could be asked to assess a compliance program, grouped by topic
The Revised Guidance

- Part of a broader 2017 DOJ initiative to review policies and guidance and integrate them into the Justice Manual, as appropriate
- Assistant Attorney General Benczkowski announced the Revised Evaluation Guidance on April 30, 2019
- Per AAG Benczkowski, the Revised Evaluation Guidance is intended to assist DOJ prosecutors in their appraisal of corporate compliance programs in making:
  - Charging decisions
  - Sentencing recommendations
  - Decisions as to the imposition of compliance monitor
- DOJ Compliance Counsel position no longer exists
Key modifications to the Evaluation Guidance

- Modifications to the structure and tone of the Evaluation Guidance
- Alignment with the Justice Manual, U.S. Sentencing Guidelines and other Department policy
- The re-issue does not represent a major modification in policy or approach by the DOJ to its assessment of compliance programs
- Reorganizes the document thematically and integrates additional details and clarifications
Three fundamental questions

- Three "fundamental questions" concerning corporate compliance:
  - *Is the corporation’s compliance program well designed?*
    - Risk assessment, policies and procedures, training and communications, confidential reporting and investigation, third party management, M&A
  - *Is the program being applied earnestly and in good faith? In other words, is the program being implemented effectively?*
    - Commitment by senior/middle management, autonomy and resources, incentives and disciplinary measures
  - *Does the corporation's compliance program work in practice?*
    - "Root cause" analysis and remediation, continuous improvement and periodic testing, investigation of misconduct
Key takeaways – DOJ and OFAC Compliance Expectations

- Increasing trend towards prescriptive compliance expectations
- Common themes
- Existing compliance infrastructure can be leveraged in a coordinated way to meet newly published expectations
- Document, test and measure compliance program to demonstrate adherence to expectations
- Effective corporate compliance is tailored to each company and its unique risk profile, not just these documents
Cross-Border Investigations Issues
When investigating sanctions issues, relevant information (documents, communications, etc.) is often located outside of the U.S. where the relevant conduct occurred or a relevant party is located.

A number of issues must be considered in a global environment:

- **Privilege**: Application of attorney-client privilege and attorney work product doctrine varies across jurisdictions; important to understand differences to ensure protection of investigation materials form disclosure to third parties ("Touch Base" Test)

- **Data Privacy**: Varying privacy regimes across the globe will impact the conduct of the investigation as well the production of materials to regulators

  - engage local resource before conducting email or document reviews
Additional issues for consideration in a global setting:

- **Employment Law**: Careful attention must be paid to rights of employees in the course of the investigation as well as in consideration of potential adverse action.
- Inability to terminate an employee who has engaged in misconduct due to local employee rights laws could impact a regulator's or enforcement body's view of remediation efforts.

- **Cultural Differences**: Cultural differences will impact approach to the conduct of an investigation; e.g., in some cultures, candor in discussions with regulators is not the norm.

- **Managing Multiple Regulators**: Depending on the nature of the conduct and the relevant jurisdiction, decisions on regulatory notices and management will be critical; different cooperation expectations; information sharing among multiple regulators; potential for conflicting strategies in dealing with different authorities; self-disclosure considerations more complicated; global settlements – DOJ policy against piling up.

- **Securing Evidence**: data storage locations and approach; privacy and state secrets considerations.
Additional Issues To Consider In a Global Setting

- Additional issues for consideration in a global setting:
  - Blocking statutes -- notably, France and Switzerland
  - Bank secrecy laws -- may make it a criminal offense to disclose information subject to secrecy regulations, e.g., an account holder's identity
  - State secrets and national security laws, e.g., in China
  - Data residency requirements
Export Control and Economic Sanctions Enforcement Developments
2019 YEAR-END REVIEW of Import/Export Developments

bakermckenzie.com

Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2019 Baker & McKenzie LLP