GIBSON DUNN

December 5, 2019

NEW GUIDANCE ON INTERNAL COMPLIANCE PROGRAMS ("ICPS") – WHAT REGULATORS ON BOTH SIDES OF THE ATLANTIC EXPECT FROM INTERNATIONAL BUSINESS

To Our Clients and Friends:

The European Union has become more active in addressing EU common foreign and security policy ("**CFSP**") objectives with the help of what it calls "restrictive measures," i.e., EU Financial and Economic sanctions. As indicated in our recent client alert, *The EU Introduces a New Sanctions Framework in Response to Cyber-Attack Threats* and even more recent by introducing a framework for EU Financial Sanctions against Turkey,[1] it has also specifically started to unilaterally implement sanctions addressing EU security concerns, including issues beyond traditional areas addressed by sanctions such as "traditional" sanctions imposed due to terrorism and international relations-based grounds. We have discussed this development and respective challenges in our recent publication *U.S., EU, and UN Sanctions: Navigating the Divide for International Business.*[2]

Furthermore, the EU Commission started to become more vocal on how it expects individuals and companies under its jurisdiction to implement those restrictive measures. A good example is the detailed guidance provided with regard to the EU Blocking Statute.

As shown below, the EU Commission has moved forward now and published the EU Guidance on Internal Compliance Programmes ("**ICPs**") for dual-use trade controls.[3] In the following, we shall highlight key recommendations of the EU guidance and some additional points we consider helpful. Please note that the competent authorities of EU member states might have additional requirements and expectations.[4]

In some respects, these developments in the EU mirror recent developments in the United States. The U.S. Department of Commerce Bureau of Industry and Security ("**BIS**") has previously published compliance guidance for the export of dual-use items that closely tracks the EU Commission's guidance on ICPs.[5] The EU guidance also references similar advice on internal compliance programs published by the U.S. Department of State.[6] Most recently, the Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), which administers U.S. sanctions, has published guidance on sanctions compliance best practices, advising companies to implement compliance programs with similar central features. For companies with an U.S. nexus, we suggest additionally reviewing these resources, as well as our recent client alert OFAC Releases Detailed Guidance on Sanctions Compliance Best Practices.

1. EU Commission recommendations on internal compliance programs

The guidance issued by the EU Commission is intended to support companies with applying a framework *to identify, manage and mitigate risks associated with dual-use trade controls and to ensure compliance with the relevant EU and national law and regulations*[7].

The guidance consists of seven core elements representing what the EU Commission believes should be the "cornerstones"[8] of a company's individual ICP.[9] While it notes that there is no one-size-fits-all approach, it also notes that "*A company's approach to compliance that includes policies and internal procedures for, at least, all the core elements could be expected to be in line with the EU ICP guidance for dual-use trade controls.*"[10]

While the focus of the guidance is on managing dual-use trade[11] control impact and mitigating associated risks[12], we believe it also sheds a light on general expectations the EU Commission has with respect to internal compliance programs regarding sanctions and export controls.

1.1 Risk assessment

Prerequisite for the installation of an ICP is an assessment of the company's business activities and their related risk of violating EU export controls, specifically the dual-use regulations. Rather than identifying every single exposure to EU regulation, this risk assessment serves as a basis to design an ICP tailor-made for the company.[13]

Furthermore, we suggest that in case the risk profile changes, such risk assessment should be rerun and—if deemed necessary—the ICP should be revised to fit the changed risk profile.

1.2 Top-level management commitment to compliance

The top-level management should continuously and distinctly express their commitment to a culture of compliance in order to lead by example. Regularly communicating corporate commitment to compliance to all employees and defining expectations, both orally and in writing, is considered vital in order to encourage such a culture of compliance.[14]

We further suggest such making sure this commitment—including the way it was expressed—is well-documented.

Furthermore, any expressed commitment to compliance should be reviewed by counsel to ensure the statement itself does not cause regulatory concerns in light of applicable anti-boycott law. For example, a statement made by a German resident noting, "*Our company fully complies with all U.S. sanctions,*" is itself a breach of applicable law in Germany, specifically section 7 of the German Trade Ordinance.

1.3 Organization structure, responsibilities and resources

According to the EU guidelines, companies should create an internal organizational chart in order to define responsibilities and assign functions to various employees. It is also suggested that companies

designate at least one person in control of the overall compliance commitment (in some EU Member States this person must be part of the top-level management)and at least one employee in charge of the dual-use trade control function.[15] The personnel overseeing compliance with dual-use regulations needs to be authorized to stop transactions and has to be guarded from potential conflicts of interest.

Additionally, companies are advised to give these personnel access to relevant legislation, especially the latest lists of controlled goods and embargoed or sanctioned destinations and entities, and to gather all relevant compliance-related documents (policies and procedures) and assemble them in a "compliance manual."

1.4 Training and awareness raising

Companies should also require periodic training (in the form of external seminars or in-house training events, etc.) to keep the control staff up-to-date with the dual-use regulations and the company's ICP.[16] Training sessions may also include lessons learned from performance reviews. Moreover, as potential compliance issues are a concern at all relevant levels of a company, measures to raise awareness for such issues should be taken accordingly.

1.5 Transaction screening process and procedures

Establishing standardized transaction processes and procedures can help ensure compliance with relevant export law. This is best achieved by collecting and analysing all relevant information concerning item classification, transaction risk assessment, license determination and post-licensing controls.[17]

Even if all necessary information is readily available, it remains challenging to verify a certain item classification from a legal perspective as the performance characteristics of an item need to be checked against the EU and national dual-use control lists. This classification regularly demands cooperation between different departments of a company, such as a cooperation between the competent technical department and the legal team.[18]

Companies may also directly contact the competent authority and ask for assistance with the classification after providing a detailed technical description of the respective item. At the competent authorities, such mix of personnel is mirrored, e.g. the competent German authority, the *Federal Office for Economic Affairs and Export Control* (*BAFA*), employs both (legally trained) engineers / technicians and lawyers.

1.6 Transaction risk assessment

Companies also need to ascertain whether their counterparties (intermediaries, purchasers, consignees or end users) are subject to any embargoes or sanctions. The guidance of the EU Commission proposes acquiring end-use statements from customers, checking the reliability of end users with the national competent authority and to giving attention to diversion risk indicators. If information learned or acquired from the competent authority gives cause for concern, procedures must be in place to avert any export without the authority's explicit permit.[19]

1.7 Licensing

The company should ensure that it has all relevant contact details of the competent control authority. Moreover, the exporter should be aware that exports via cloud services or personal baggage and other activities such as providing technical assistance and brokering are subject to dual-use control measures.[20]

1.8 Post-licensing controls

A final check should be conducted to make sure that all steps ensuring compliance were duly taken and that licenses have not been invalidated since their issuance due to changes of the details of the exporter, the intermediaries or the end users.[21] A procedure to stop or suspend the export—if necessary—should be implemented. Note that companies are still obligated to independently investigate the lawfulness of the transaction.[22]

1.9 Performance review, audits, reporting and corrective actions

According to the guidelines, it is essential to implement procedures that regularly analyse, test, evaluate, and revise the company's ICP (e.g., in the form of targeted and documented audits).[23] Furthermore, specific reporting procedures should be in place in order to enable the company to take the required action when a case of noncompliance is suspected or has occurred. Employees must also feel secure to express concerns about noncompliance or the operational reliability of the ICP. Any suspected noncompliance should be documented. After taking effective corrective actions, the relevant personnel should be informed of those measures.

1.10 Record-keeping and documentation

The company should establish policies for legal document storage, record management and traceability of trade control-related activities.[24] This may be legally required in some cases, but it also generally renders the search for legal documents more effective. The relevant EU and national legal provisions for record-keeping (period of safekeeping, scope of documents, etc.) should be reviewed before establishing such a filing system. Additionally, it is suggested that the company keep track of past contacts with responsible authorities.

1.11 Physical and information security

Due to the generally high sensitivity of dual-use items, companies are requested to introduce procedures to prevent the unapproved access to and removal of controlled items. With regard to physical items, the establishment of restricted access areas, personnel access or exit controls or physically safeguarding the respective item should be considered. To assure the security of physically intangible technology, the guideline recommends, among other steps, that the company install antivirus programs, file encryption and firewalls[25].

2. Outlook

Taking into account both the new EU guidance and the Framework for OFAC Compliance Commitments,[26] there is a clear trend visible from authorities to voice and detail their expectations on how companies should address sanctions and export control compliance. In turn, it can be expected that noncompliance with such expectations will increasingly be under enhanced regulatory scrutiny.

---

[1] See: Press release of the Council of the EU: *Turkey's illegal drilling activities in the Eastern Mediterranean: Council adopts framework for sanctions*, available online at: https://www.consilium.europa.eu/en/press/press-releases/2019/11/11/turkey-s-illegal-drilling-activities-in-the-eastern-mediterranean-council-adopts-framework-for-sanctions/.

[2] A. Smith, S. Connor and R. Roeder, *U.S., EU, and UN Sanctions: Navigating the Divide for International Business*, Bloomberg, 2019, ISBN 978-1-68267-281-5. The first chapter can be found online at: https://www.gibsondunn.com/wp-content/uploads/2019/11/Smith-Connor-Roeder-US-EU-and-UN-Sanctions-Navigating-the-Divide-for-International-Businesses-Bloomberg-Law-2019.pdf.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 3/18.

[4] E.g. for Germany, please see: *Internal Compliance Programmes – ICP - Company-internal export control systems*, available online at: www.bafa.de › Downloads › afk_merkblatt_icp_en.

[5] https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file.

[6] https://icp.acis.state.gov/.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 1/18.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 3/18.

[9] Please note that the EU ICP guidance makes reference to the 2011 Wassenaar Arrangement Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies (available online at https://www.wassenaar.org/app/uploads/2015/06/2-Internal-Compliance-Programmes.pdf); the "Best Practice Guide for Industry" from the Nuclear Suppliers Group (NSG), *click here*; the ICP elements in the Commission Recommendation 2011/24/EU; the results from the fourth Wiesbaden Conference (2015) on "Private Sector Engagement in Strategic Trade Controls: Recommendations for Effective Approaches on United Nations Security Council Resolution 1540 (2004) Implementation"; and the 2017 United States Export Control and Related Border Security Program ICP Guide website (available online at http://icpguidelines.com/).

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 3/18.

[11] Council Regulation (EC) 428/2009, regularly referred to as the EU Dual-Use Regulation, has set up an EU regime for the control of export, transit and brokering of dual-use items in order to contribute to international peace and security by precluding the proliferation of nuclear, chemical, or biological weapons and their means of delivery. To adapt to the rapidly changing technological, economic and political circumstances, the EU Commission presented a proposal in September 2016 to update and expand the existing rules that was supported by the European Parliament in its first report on the matter. On June 5, 2019, the Council issued its own parameters for negotiations with the European Parliament seeking a more limited recast of the dual-use regulation. Thereby the discussion mainly focuses on the classification of cyber surveillance technologies as dual-use goods and the possibility of a resulting discrimination of EU companies. Considering the ongoing discussions, we do not expect the implementation to take place in the coming weeks. The progress of the respective discussion can be viewed at : http://www.europarl.europa.eu/legislative-train/theme-europe-as-a-stronger-global-actor/file-review-of-dual-use-export-controls.

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 3/18.

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 4/18.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – pages 5/18 and 6/18.

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 6/18.

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 7/18.

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 7/18.

[18] For best practices from a company perspective please see: Müller, Alexandra / Groba, Alexander in AW-Prax 2019 – page 300.

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 9/18.

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 10/18.

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 10/18.

[22] Müller, Alexandra / Groba, Alexander in AW-Prax 2019 – page 303.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 10/18.

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 11/18.

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN – page 12/18.

[26] https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Patrick Doris, Michael Walther, R.L. Pratt and Richard Roeder.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's International Trade practice group:

United States:

Judith Alison Lee - Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Ronald Kirk - Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
Jose W. Fernandez - New York (+1 212-351-2376, jfernandez@gibsondunn.com)
Marcellus A. McRae - Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Adam M. Smith - Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Stephanie L. Connor - Washington, D.C. (+1 202-955-8586, sconnor@gibsondunn.com)
Christopher T. Timura - Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com)
Ben K. Belair - Washington, D.C. (+1 202-887-3743, bbelair@gibsondunn.com)
Courtney M. Brown - Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com)
Laura R. Cole - Washington, D.C. (+1 202-887-3787, lcole@gibsondunn.com)
R.L. Pratt - Washington, D.C. (+1 202-887-3785, rpratt@gibsondunn.com)
Samantha Sewall - Washington, D.C. (+1 202-887-3509, ssewall@gibsondunn.com)
Audi K. Syarief - Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com)
Scott R. Toussaint - Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com)

Europe:

Peter Alexiadis - Brussels (+32 2 554 72 00, palexiadis@gibsondunn.com)
Nicolas Autet - Paris (+33 1 56 43 13 00, nautet@gibsondunn.com)
Attila Borsos - Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Patrick Doris - London (+44 (0)207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly - London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Steve Melrose - London (+44 (0)20 7071 4219, smelrose@gibsondunn.com)

Benno Schwarz - Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder - Munich (+49 89 189 33-160, rroeder@gibsondunn.com)