EU to impose stricter export controls on cyber-surveillance items

By Mario Mancuso, Esq., Anthony Rapa, Esq., and Anais Bourbon, Esq., Kirkland & Ellis

JUNE 15, 2021

Following the Council of the European Union's (Council) adoption of an updated regulation on May 10, 2021 (Updated Regulation), the European Union (EU) is set to expand its Dual-Use Regulation (Council Regulation (EC) No 428/2009, as amended) to authorize restrictions on exports of items that could be used to support human rights abuses, with a focus on "cyber-surveillance items," among other changes.

The regulation is expected to be published in the EU Official Journal shortly and will enter into force 90 days thereafter.

'Cyber-surveillance' items

The Updated Regulation targets "cyber-surveillance items," defined as dual-use items "specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data from information and telecommunication systems." *(Definition Art. 2(20))* Such items already may be listed in Annex I of the Dual-Use Regulation, in which case they already are subject to an export licensing requirement. However, with respect to *unlisted* cyber-surveillance items (*i.e.*, items that are the equivalent of "EAR99" under the U.S. rules), under the Updated Regulation such items can be subject to a licensing requirement under the following circumstances:

- There will be a licensing requirement if the company is informed by a Member State that the items are or may be intended for use in connection with human rights violations and/or internal repression. *(Art 5(1))*
- Exporters that become aware that cyber-surveillance items may be intended for such purposes will be required to notify the relevant authority, which then will decide whether to impose a licensing requirement. *(Art.5(2))*
- The Updated Regulation allows individual Member States to impose a licensing requirement for unlisted cyber-surveillance items if the exporter has "grounds for suspecting" that these are or may be intended for any use in human rights violations and/or internal repression. *(Art. (53))*

Where a Member State imposes a licensing requirement as described above, it is required (with narrow exceptions) to notify other Member States, which then must give "due consideration" to the information received. The Updated Regulation further provides that where all Member States notify the European Commission (Commission) that an export authorization requirement should be imposed for "essentially identical transactions," the Commission shall publish in the Official Journal of the European Union information regarding the cyber-surveillance items and restricted destinations. *(Art 5(6))* Additionally, Member States are required to consider proposing to multilateral export control regimes that such items be controlled.

Furthermore, in a measure praised by civil society groups, the Updated Regulation requires the Commission to submit an annual report to the European Parliament and the Council detailing, inter alia, the number of export license applications for cyber-surveillance items on a per-item basis; the issuing Member State; the relevant countries of destination; and the decisions taken on those license applications. *(Art. 12(2))*

Cooperation between member states

The Updated Regulation expands information sharing and cooperation between Member States regarding controls of certain items impacting "public security," including with respect to anti-terrorism and human rights issues.

Specifically, pursuant to this, the Updated Regulation authorizes Member States to control EU-unlisted items on their own national control lists for reasons of "public security, including the prevention of acts of terrorism, or for human rights considerations." *(Art 9)* In such cases, Member States are required to notify the Commission of the reasons and the export requirements, which will be published in the EU Official Journal *(Art 9.3-9.4; Art 26.2)*. The Commission shall publish a compilation of national control lists in force throughout the Member States.

Notably, following enactment of controls by one Member State under the procedures described above, an export license may be required by another Member State if that Member State imposes controls on identical items and informs the exporter of such. *(Art 10)*. Where a Member State takes such action, other Member States are required to give "due consideration" of such information and inform their customs authorities accordingly.

Technical assistance

The Updated Regulation includes new controls on technical assistance with respect to listed dual-use items that are or may be intended for use in connection with chemical, biological, or nuclear

weapons, or for military end-use if the country of destination is subject to an arms embargo.*(Art 4.1; 8.1)* If the provider of technical assistance is aware that the items may be intended for such purposes, it is required to notify the relevant authority, which will decide whether an authorization is required. *(Art 8.2)*.

Notably, "technical assistance" is broadly defined as "any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including by electronic means as well as by telephone or any other verbal forms of assistance."

New general export authorizations

The Updated Regulation somewhat expands certain existing general export authorizations (*i.e.,* license exceptions), and also sets out the following two new general export authorizations:

- **Exports to subsidiaries and affiliates**: Union General Export Authorization EU007 allows exports of controlled software and technology to the exporter's subsidiaries and affiliates based in Argentina, Brazil, Chile, India, Indonesia, Israel, Jordan, Malaysia, Mexico, Morocco, the Philippines, Singapore, South Africa, South Korea, Thailand, and Tunisia. *(Annex II G.)*. (Notably, preexisting authorizations already broadly authorize exports to core EU allies such as the United States, Canada, Australia, and Japan, among others.) Certain specified sensitive items, however, are not eligible for export under the general authorization.
- **Encryption items**: Union General Export Authorization EU008 allows export of certain encryption and cryptographic items to all destinations, excluding certain listed countries and subject to certain conditions, unless the exporter has been informed that the items are or may be intended for use in connection with chemical, biological, or nuclear weapons; a military, police, or surveillance end-use; or violations of human rights, democratic principles, or freedom of expression. *(Annex II H . Encryption, Part 3. conditions)*. Excluded countries include China (including Hong Kong), Russia, Israel, Iran, Syria, Belarus, and the United Arab Emirates, among others. The promulgation of this general authorization is a notable step towards the sort of broad authorization for encryption exports set out in the U.S. License Exception "ENC."

Internal compliance program (ICP)

The Updated Regulation requires exporters using or applying for global export authorizations (*i.e.,* specific licenses authorizing a category of exports to various end-users and countries) to implement a formal ICP. An ICP is defined as "ongoing effective, appropriate and proportionate policies and procedures" to facilitate compliance with the Dual-Use Regulation, including due diligence of end-uses and end-users. *(Definition Art.2 (21))*.

Key takeaways

- Companies should prepare for export restrictions on cyber-surveillance items that may be used in connection with human rights abuses.
- It will be important to monitor related developments in the United States, where similar efforts are underway to link export controls to human rights considerations.
- The annual reporting requirement figures to provide a measure of transparency regarding EU exports of cyber-surveillance items, a subject of extensive commentary in recent years.
- New general authorizations permit certain intra-group exports and certain exports of encryption items.
- Companies using global export authorizations, or applying for such authorizations, will need to implement an ICP if they do not have one in place already.
- Technical assistance involving dual-use items for certain sensitive end-uses may be subject to an authorization requirement.

About the authors



Mario Mancuso (L) is a partner in **Kirkland & Ellis'** Washington, D.C., office and leads the firm's international trade and national security practice. His practice focuses on guiding private equity sponsors and companies through the CFIUS process and resolving crises involving economic sanctions and export control-related investigations by the U.S. government. He can be reached at mario.mancuso@kirkland.com. **Anthony Rapa** (C), a partner in the firm's Washington, D.C., office, counsels companies and private equity sponsors regarding economic sanctions and export control issues in the context of corporate transactions and internal investigations. He can be reached at anthony.rapa@kirkland.com. **Anais Bourbon** (R), an associate in the firm's Washington, D.C., office, advises companies on complex-cross border transactions, regulatory matters and investigations relating to U.S. national security, economic sanctions, export regulations and European analogues. She can be reached at anais.bourbon@kirkland.com.

This piece was first published on Reuters Legal News and Westlaw Today on June, 15, 2021.