



IPC Briefing on the EU Dual-Use Export Controls Regulation

April 2018

Executive Summary

The EU is currently working to update its Regulation on export controls for dual-use items, meaning items that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD).

As the proposal now stands, it is likely to impact the electronics industry in the following areas:

- Expansion of list of dual-use items to include cyber-surveillance technologies and those that can be used for human rights violations.
- Added obligation for exporters, when conducting their due diligence, to notify Member State authorities, if they suspect exported items not listed in the Regulation are used to violate human rights.
- The European Commission is empowered to amend the list of dual-use items covered by the Regulation, so continuous monitoring of this process will be needed to ensure regulatory compliance.

The Dual Use Export Controls Regulation

Dual-use items refers to goods, software and technology that can be used for both civilian and military applications and/or can contribute to the proliferation of Weapons of Mass Destruction (WMD). Trade in such goods is subject to controls to prevent the risks that these items may pose for international security. Such controls derive from international obligations (e.g. relevant United Nations resolutions) and the EU is thus controlling the export, transit and brokering of dual-use items as a key instrument contributing to international peace and security.

The EU export control regime is currently governed by [Regulation \(EC\) No 428/2009](#), which provides for common EU control rules, a common EU list of dual-use items (p. 12 onwards in the previous link), as well as coordination and cooperation to support consistent implementation and enforcement throughout the EU. A proposal to modernize this regulation (Recast) was published by the European Commission in September 2016 (more on the state of play below) and is currently under discussion by the co-legislators (the European Parliament and the Council of the EU).

Proposal for a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (Recast)

In the debate preceding the proposed update of the dual-use export controls regulation, the preferred option was for a combination of "EU system upgrade" (adjustments to the regulatory framework), and "EU system modernization" (focusing on cyber-surveillance Technologies and human rights). With that in mind, the proposal put forward the following provisions:



Control provisions:

- the definition of dual-use items is revised to reflect the emergence of new types of dual-use items, such as **cyber-surveillance** technologies. The proposal also clarifies that controls apply to natural persons, who may be "exporters", especially when it comes to technology transfers (more details on cyber-surveillance technologies can be found below);
- the proposed regulation seeks to harmonized so-called "**catch-all**" provisions, meaning cases where Member States can use an "emergency brake" in the export of an item, if they suspect possible misuse. Criteria for activating this brake are terrorism and human rights violations, while the export of cyber-surveillance technology is also covered.
 - There have been some concerns by industry stakeholders that the conditions of use of catch-all provisions is not sufficiently defined, with calls for a list of excluded end-users to be provided by the European Commission to help industry compliance.
- clarifies controls on and facilitates **intangible technology transfers**, as they only become subject to control when the dual-use technology is made available to a person in a third country;
- clarifies controls applicable to **technical assistance** involving a cross-border movement;
- strengthens **brokering controls**, (i) by extending the definition of the broker to subsidiaries of EU companies outside of the EU, as well as to brokering services supplied by third country nationals from within the EU territory; (ii) by harmonising their application to non-listed items and military end-uses and extending their application to **terrorism and human rights violations**;
- harmonises the application of transit controls to non-listed items and military end-uses, and extends controls to the risk of misuse for terrorist acts and human rights violations;
- puts in place certain controls an anti-circumvention clause to combat trafficking in items of dual usage.

EU licensing:

- establishes a **new authorisation for 'large-projects'** for certain large multiannual projects e.g. construction of a nuclear power plant;
- introduces **new general authorisations regarding encryption and low value shipments** to facilitate trade while ensuring a sufficient level of security (e.g. registration, notification and reporting, and auditing);
- introduces a general authorisation on **intra-company transfers of dual-use technology** in non-sensitive countries, in particular for research and development purposes, as long as the technology remains under the ownership or control of the parent company.

Re-evaluation of intra-EU transfers: the proposal revises the [list of items](#) subject to control within the EU in order to focus controls on an updated list of most sensitive items, taking account of technological and commercial developments.

Control of exports of cyber-surveillance technologies: the proposal sets out new provisions for an effective control focusing on specific and relevant cyber-surveillance technologies. It introduces an [EU autonomous list](#) (p. 243-244) of specific cyber-surveillance technologies of concern to be subject to controls (monitoring centres and data retention systems), with detailed technical parameters.

- Under the proposed regulation "'cyber-surveillance technology' shall mean items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analyzing data and/or incapacitating or damaging the targeted system." It includes items related to mobile telecommunication interception equipment; intrusion software; monitoring centers; lawful interception systems and data retention systems; digital forensics.
- **Some stakeholders have expressed concerns that the definition of cyber-surveillance technologies is too broad and could risk including numerous essential and legitimate defensive security products and services.**



The proposal will also expand the European Commission's power to amend lists of dual-use items and general export authorizations to make the system more flexible and responsive to technological or economic developments.

European Parliament position

In January 2018 the European Parliament adopted its position on the proposed regulation and agreed to use this position as the basis for negotiations with the Council of the EU and the Commission to reach a final agreement. MEPs decided to strengthen certain aspects of the proposal, most notably the following:

- Cover technology used for cyber-surveillance and human rights violations (e.g. right to privacy and data protection, freedom of expression, freedom of assembly and association).
- Exporter due diligence, obliging exporters to notify national authorities, in the event they become aware that products not included in the Regulation may be intended to violate human rights.
- A Member State may prohibit or impose an authorization requirement on the export of dual-use items not listed in the Regulation for reasons of public security, for human rights considerations or for **the prevention of acts of terrorism**.
- When evaluating export authorization on cyber surveillance items, Member States must take into account the risk of violation of the right to privacy, the right to data protection, freedom of speech and freedom of assembly and association, as well as risks relating to the rule of law.
- Encryption technologies should be removed from the list of controlled items.

Importance for IPC members

Dual-use export controls affect research and development (R&D), production and trade of typically high-tech, advanced products across a wide-range of industries – including aerospace, defense and security, telecommunications and information security, chemical pharmaceutical industries, material-processing equipment, electronics, semiconductor and computing industries, lasers and navigation.

As IPC members would already be abiding by the existing dual-use controls regime, the main impact of this regulation would be the expansion into cyber-surveillance technologies and those that can be used for human rights violations.

In addition, there is an added obligation imposed on exporters, when conducting their due diligence, to notify Member State authorities, if they suspect exported items not listed in the Regulation are used to violate human rights.

Finally, it would be necessary to continue monitoring for delegated acts amending the Annex of the Regulation, where a list of dual-use products subject to controls will be listed.

Next steps

The proposal is currently under discussion in trilogue negotiations, which are informal meetings of representatives of the Parliament, Council of the EU and European Commission to reach an agreement on the legislative proposal. Once agreement is reached in trilogue, a proposal is usually formally adopted soon after.

It will enter into force on the ninetieth day after its publication on the official journal of the EU and will be directly applicable in all Member States.

About IPC

IPC is the world's leading association for electronics manufacturing companies, representing the printed circuit board and electronics assembly industries, their customers and suppliers worldwide. With global headquarters in the US and



regional offices in Europe and China, IPC's European membership includes large companies, such as Airbus and Siemens, but also a vast array of small and medium enterprises (SMEs).

We welcome the feedback of IPC members on dual use export controls. Should you have any comments or need more information, you can visit www.ipc.org/advocacy or contact:

Chris Mitchell
Vice-President of Global Government Relations
IPC- Association Connecting Electronics Industries
1331 Pennsylvania Avenue, Suite 910
Washington, DC 20004
+1 (202) 661-8092
ChrisMitchell@ipc.org