AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Control of exports, transfer, brokering, technical assistance and transit of dual-use items (RECAST)

How would the European Parliament's position impact businesses?

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

The American Chamber of Commerce to the European Union (AmCham EU) supports the aim of the recast of the EU's Regulation on the export control of dual-use items, as it tries to ensure that certain goods and technologies are not used by rogue actors to commit human right violations. However, as it currently stands, the proposed revision of the regulation would only apply additional controls under often vague and ill-defined conditions. This could lead to significant regulatory uncertainty for industry and harm the competitiveness of the European market. Moreover, the creation of unilateral regimes at EU level could cause disruptions to global value chains and further fragment the international regulatory space for companies, as they would have to comply with increasingly diverging dual-use export regimes.

The below paper analyses the position of the European Parliament on the dual-use items recast and considers how the proposed regulation could impact businesses.

Recital 17 – Unilateral EU lists

'Decisions to update the common list of dual-use items subject to export controls in Section A of Annex I should be in conformity with the obligations and commitments that Member States and the Union have accepted as members of the relevant international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties. Decisions to update the common list of ***cyber-surveillance*** *items subject to export controls in Section B of Annex I, should be made in consideration of the risks that the export of such items may pose as regards* ***their use for*** *violations of* ***international*** *human rights* ***law*** *or international humanitarian law* ***in countries where such violations, especially regarding the freedom of expression, the freedom of assembly and the right to privacy, have been established****, or the essential security interests of the Union and its Member States. Decisions to update the common list of dual-use items subject to export controls in Section B of Annex IV should be made in consideration of the public policy and public security interests of the Member States under Article 36 of the Treaty on the Functioning of the European Union. Decisions to update the common lists of items and destinations set out in Sections A to J of Annex II should be made in consideration of the assessment criteria set out in this Regulation.* ***Decisions to delete entire subcategories on cryptography and encryption, such as in Category 5 of Section A of Annex I or as in Section I of Annex II should be made in consideration of the Recommendation of 27 March 1997 of the OECD Council concerning Guidelines for Cryptography Policy****.'*

The amendment broadens the scope for when an item can come under consideration for listing. By providing express reference to the 'freedom of expression', the 'freedom of assembly' and the 'right to privacy', the Parliament greatly increases the scope of the article. The inclusion of rights, such as 'right to privacy' could prove difficult for competent authorities to determine. Considering that licencing decisions are taken in the export control departments, it could be argued that these bodies do not have the adequate information to take decisions of whether these rights have been or will be infringed upon. The creation of unilateral regimes at EU level could harm the global competitiveness of European industry and ignore existing international export control regimes. Failure to successfully negotiate such technology to be controlled by the recognised international regime (ie. Wassenaar) is unlikely to see a significant decrease in human rights violations, as the relevant cyber surveillance technology could alternatively be procured and exchanged outside of the EU.

A positive development in the Parliament's amended version is the inclusion of a deletion mechanism for cryptography and encryption. This gives recognition to the fast-paced nature of these technologies and the necessary flexibility they require.

Article 2 (1.1.b) – Cyber-surveillance definition

> *'cyber-surveillance* ***items including hardware, software and*** *technology,* ***which are specially designed to enable the covert intrusion into information and telecommunication systems and/or the monitoring, exfiltrating, collecting and analysing of data and/or incapacitating or damaging the targeted system without the specific, informed and unambiguous authorisation of the owner of the data, and which can be used in connection with the violation of human rights, including the right to privacy, the right to free speech and the freedom of assembly and association, or*** *which can be used for the commission of serious violations of human rights* ***law*** *or international humanitarian law, or can pose a threat to international security or the essential security of the Union and its Members.* ***Network and ICT security research for the purpose of authorised testing or the protection of information security systems shall be excluded;'***

The proposed definition for cyber-surveillance technology is clearly a step in the right direction, as it provides vital limitations to what would fall under the definition of cyber-surveillance items. With its focus on covert intrusions and unauthorised data processing, policy-makers have been able to improve the definition from the Commission proposal, which had not been proportionate to the objective of the dual-use export regime. Moreover, the clear exclusion of network and ICT security research from the scope of the controls is a significant improvement.

To ensure that there is consistency between the definition and the annex, any explanation of what covert intrusion is has to include not only the consent of the data owner but also that of the owner and administrator of the relevant systems. Moreover, any definitions considered for inclusion in the controls must be developed in consultation with the cybersecurity community. This will ensure that they do not inadvertently restrict exports of items used for legitimate purposes, such as information security testing or cyber incident response, which could result in disproportionate harm to privacy and data security objectives.

Article 4 (2) – Catch-all clause

> *'If an exporter,* ***becomes aware while exercising*** *due diligence* that dual-use items* ***not listed in Annex I*** *which he* ***or she*** *proposes to export,* ***may be*** *intended, in their entirety or in part, for any of the uses referred to in paragraph 1, he* ***or she*** *must notify the competent authority* ***of the Member State in which he or she is established or resident in****, which will decide whether or not it is expedient to make the export concerned subject to authorisation*.'
>
> **'****due diligence' shall mean the process through which enterprises can identify, prevent, mitigate and account for how they address their actual and potential adverse impacts as an integral part of business decision-making and risk management systems;*** *(Article 2 (1.23a)*

Article 4 significantly expands the scope of the catch-all clause with the inclusion of human rights concerns as a trigger for controls. This would oblige exporters to seek an export license when they become 'aware' that items they purport to export are or may be intended for human rights violations. While the need for human rights safeguards is undisputed, this article places an undue burden on exporters as it exponentially expands the extent of due diligence expected of them with respect to proposed exports of non-listed items. Without a clear definition of when the awareness threshold is, and what level of due diligence is required, it will be difficult for exporters to define when a notification must be made.

The burden of making these decisions should not be placed on industry, but instead, notification and licencing guidance should be introduced by government authorities. This could be achieved via customs authorities, who are much better equipped to identify destinations and end users posing a human rights risk, and alert industry of such risks. The introduction of a base-level harmonised EU list of parties and end-users of concern could provide additional support for government authorities and certainty for industry.

An overly prescriptive approach, however, could have negative implications, as it is often preferable to maintain flexibility when exercising due diligence. This allows for a proportional approach that is tailored to the facts and circumstance of specific transactions.

Moreover, human rights concerns that are identified through due-diligence procedures, should be based on parameters that are already enforced by industry when undergoing their due-diligence checks. Any additional requirement within Article 4(2), could otherwise impose significant new due diligence checks and notification requirements, without actually improving the identification of human rights concerns.

Article 24 (2.2) – Information requirements

> *'Member States shall provide to the Commission all appropriate information for the preparation of the report. This annual report shall be public.* ***Member States shall also disclose publicly, at least quarterly and in an easily accessible manner, meaningful information on each license with regard to the type of license, the value, the volume, nature of equipment, a description of the product, the end user and end use, the country of destination, as well as information regarding approval or denial of the license request. Commission and Member States shall take into account the legitimate interests of natural and legal persons concerned that their business secrets should not be divulged****.'*

Article 24, while clarifying the nature of the information that will require sharing, also greatly expands the scope of the original Commission proposal by increasing the cycles of data to be shared by the Member States.

While greater clarity is welcome, much of the data requirements that have been added could be considered sensitive business-relevant information and therefore have considerable competition repercussions. The publication of value and volume data is seen as business critical data. Even with the safeguard of the last sentence, the Member States and the Commission will need to be considerate of business secrets and the competition consequences that the publication of such information carries with it.

Moreover, the Parliament amendments asks a great deal of administrative work from the Member States. Currently, the Member States have varied approaches on sharing export licencing information. While some might not share this information on a regular basis, others provide degrees of it on an almost monthly basis. However, the amount of information that is asked to be shared by the Parliament and the frequency of this exercise would amount to considerable administrative burdens for the Member States and subsequently for industry. If this exercise is not carried out in a harmonised way across Member States, this could create distortions within the EU and create imbalances.