COMMENTS

Guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) No. 2021/821

Brussels, 9 juin 2023

Introduction

The European Semiconductor Industry Association (ESIA) represents the Europe-based manufacturers and designers of semiconductors as well as research institutes and national associations in the field of microelectronics.

Export controls play a crucial role in semiconductor trade, given that many semiconductor industry products are classified as dual-use, with, as a consequence, the need to obtain export licenses.

ESIA is thankful to the European Commission for providing our industry with the opportunity to express its views on the proposed *Guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) No. 2021/821.*

General

ESIA supports the efforts by the European Commission to reform and modernise the EU export control system, including providing Guidelines that facilitate compliance by exporters and harmonised implementation of controls across all EU Member States.

ESIA observes that the draft includes a series of helpful explanations, including concrete positive lists of circumstances not entailing risk of misuse. ESIA would like to encourage the European Commission to integrate the draft Guidelines with further concrete operational clarifications and guidance to exporters. ESIA strongly recommends adding practical examples and/or case studies.

The draft Guidelines would benefit from the addition of a "process flow", e.g., a pictorial representation of the typical steps to be taken by exporters for compliance. Based on the proposed text, it is unclear what exporters should look at first: should they first look at the product, and if the product meets the definition, screen that product? We would like to point

out that the idea of screening all customers and all products would represent an excessive burdensome requirement, considering that many semiconductor companies have thousand products in their portfolios and hundreds of customers.

One of ESIA's main concerns is the lack of clarity regarding how far a company must go in performing its due diligence. ESIA recommends amending the Guidelines by including clear guidance in risk analysis. In our view, the Guidelines should help exporters in determining how to establish a risk, through a mechanism of red flags. The guidelines should be axed on a commonly understood concept of due diligence.

When it comes to "red flags", ESIA suggests making them more practical and ideally directly implementable by exporters.

Specific Comments

In the paragraphs below ESIA lists its main observations on specific articles.

1. **III.2. Potential non-listed cyber-surveillance items** *"Items used for purely commercial applications, such as billing, marketing, quality services, user satisfaction or network security, are generally considered not to entail risks for misuse as relevant under serious violations of human rights or international humanitarian law and therefore generally not subject to control under Art. 5 of the Reg."*

    ⇨ ESIA strongly welcomes the above detailed guidance regarding to which applications are considered not to entail risks for misuse as relevant under serious violations of human rights or international humanitarian law and therefore generally not subject to control under Art. 5 of Regulation (EU) No. 2021/821. Such guidance is a positive example of a clear watch-list of applications which do not entail risks.

2. *I.2.6 "Awareness" and "are intended for"*
    II.2.1. „"specially designed",,

    ⇨ ESIA suggests adding practical examples of "specially designed" and "intended for" items.

3. **II.3.2. "Commission of <u>*serious*</u> violation of human rights"**

    ⇨ For legal clarity and certainty, ESIA suggest adding a clear definition of "serious" violations. In addition, we recommend adding real-life examples, which can help exporters in daily operations.

4. **IV. Due Diligence Measures** *"2. Review the capabilities of the item in question to determine potential for misuse in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law by foreign end-users.It also includes an assessment to determine whether the product could be used as part or <u>component </u>of a system that could result in the same violations and/or misuse."*

⇨ Mentioning _components_ here seems problematic. There is a wide variety of components used in any given device. In this context, the relevant components should be those which are „_specially designed_".
In addition, it would be extremely and even excessively burdensome for exporters to perform such wide assessment. ESIA suggests making the assessment more narrow, maybe adding the idea of „_positive knowledge_".

5. **IV. Due Diligence Measures „_3. In support of competent authorities, review stakeholders involved in the transaction (including end-user and consignees such as distributors and resellers). […]. Before and during any transaction, review how the consignees and/or end-users intend to use the product or service, based on end-use statements."_**

⇨ ESIA suggests amending the Guidelines to clarify in which circumstances companies should ask for end-use statements. Should exporters ask for end-use statements only for products that meet the definiton? In addition, we recommend adding practical examples for more clarity.

6. _**IV. Due Diligence Measures 3. „Red flags [...] The end-user has** <u>**in the past exported cyber-surveillance items to countries where the use of such items has given rise to internal repression measures and/or serious violations**</u> **of human rights and international humanitarian law.**_

⇨ In ESIA's view, this seems difficult to comply with without further guidance. This provision gives rise to additional questions. We strongly recommend adding references to _sources_ of information which exporters should use.

Conclusions

ESIA supports the smooth functioning of the EU export control system facilitated by clear legislative & policy frameworks.

ESIA is ready to support the European Commission to further develop the proposed Guidelines in line with the suggestions in the paragraphs above, including by providing practical examples based on the experience and typical process-flows of the semiconductor industry.