Hughes Hubbard & Reed

EU Commission Publishes New Guidelines on Scope of Catch-All Controls and Due Diligence Requirements for Exporters of Non-Listed Cyber-Surveillance Items

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Key Takeaways:

- EU catch-all controls on Non-Listed Cyber-Surveillance Items are complex and far-reaching, therefore requiring EU exporters to conduct careful review and assessment prior to any exports of such items.
- Prior to each transaction involving Non-Listed Cyber Surveillance Items, EU exporters should classify the item, review the potential for misuse of the item for purposes of internal repression and/or serious violations of human rights and international humanitarian law, assess stakeholders involved in the transaction and prevent and mitigate potential future adverse impacts.

On 16 October 2024, the European Commission ("**Commission**"), published guidelines (the "**Guidelines**") for exports to third countries of cyber-surveillance items which are not listed in Annex I of the EU Dual-Use Regulation (Council Regulation 821/2021) but which could be used in connection with internal repression and/or serious violations of human rights and international humanitarian law (see Commission Recommendation 2024/2659). Although the Guidelines are not legally binding on European Union ("**EU**") exporters, they provide valuable clarifications regarding the **scope of the controls** and the **extent of due diligence efforts** expected with respect to exports of such items.

I. Background and Context

In 2021, the EU adopted a revised version of the EU Dual-Use Regulation, the framework defining EU common rules for the export of dual-use items (*i.e.,* items that can both have civil and military applications) outside the EU territory. The Dual-Use Regulation primarily defines "list-based" controls, and requires EU exporters to obtain an authorization from the national competent authority ("**NCA**") of their Member State prior to the export of dual-use items listed in its Annex I (Article 3). Annex I contains several cyber-surveillance items in two different categories, the export of which is subject to prior authorization by the NCA (Annex I, Categories 4 and 5).

EU Dual-Use Catch-All Controls on Non-Listed Cyber-Surveillance Items

The revised EU Dual-Use Regulation introduced new so-called "catch-all" controls on exports of cyber-surveillance items that are not listed in Annex I ("**Non-Listed Cyber-Surveillance Items**") (Article 5). While such items may have legitimate civilian uses (*e.g.,* law enforcement, network monitoring) they could present **potential for misuse** in connection with internal repression, and serious human rights as well as international humanitarian law violations. The new controls seek to ensure compliance with the international obligations and commitments of the EU and its Member States with respect regional peace, security, stability and respect for human rights and international humanitarian law.

However, the new controls on Non-Listed Cyber-Surveillance items **partly place the burden on EU exporters** to identify controlled items and assess potential for misuse based on their due diligence findings in each individual transaction. Additionally, a November 2023 Briefing Paper from the European Parliament highlighted the **risk of divergent interpretation** among the 27 Members States, including with respect to the items subject to these controls and related due diligence expectations.

Obligation to Obtain Prior Authorization by or Notify NCAs prior to Exports of Non-Listed Cyber-Surveillance Items

Recognizing the significant harm Non-Listed Cyber Surveillance Items could have if misused, the Dual-Use Regulation requires EU exporters, prior the export of such items, to:

- Obtain **prior authorization** from their NCA where they have been **informed by the NCA** of the potential for such misuse (Article 5(1)); or
- Notify their NCA where they have **identified potential misuse themselves based on their own due diligence findings** (Article 5(2)). The NCA may then decide to make the export concerned subject to prior authorization.

Member States may also adopt or maintain national legislation imposing prior authorizations for exports for which they suspect that certain items may be used for such purposes (Article 5(3)). However, to date, the scope and extent of the diligence efforts and awareness required from EU Exporters have been unclear.

II. Significant Clarifications Regarding Scope of Cyber-Surveillance Catch-All Controls and Related Due Diligence Requirements under New EU Guidelines

The Guidelines are issued consistent with the EU's obligation to provide guidance to EU exporters on how to implement the obligation in Article 5 (Article 26), as part of the "protect pillar" of the EU's Economic Security Strategy, which seeks to protect the EU from commonly identified economic security risks, by better deploying already existing tools, such as export controls. These Guidelines are based on feedback from consultations by the EU's Surveillance Technology Expert Group, as well as feedback from a public consultation held in Q2 2023.

Clarification of Definition of "Non-Listed Cyber-Surveillance Items"

Under the Dual-Use Regulation, cyber-surveillance items are generally 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." (Article 2(20).) Given the rapid evolution of such technologies, the definition is broad by design, but has in practice made it difficult for EU exporters to assess with certainty which items fall within the scope of these controls. The new Guidelines' clarifications regarding several key terms therefore provide valuable guidance for EU exporters that seek to determine whether their items are subject to the controls:

Term	Guidelines' Definition
"Specially designed"	• Means that the **covert surveillance of natural persons** must have been the **main purpose** of the development and design of the product; • Does not require that the item can solely be used for the covert surveillance of natural persons.
"Covert surveillance"	• Refers to situations where **surveillance is not obviously perceptible to the affected natural person** so that the latter does not have the opportunity to remove himself/herself from that surveillance or at least to adjust his/her behavior accordingly.
"Natural person"	• Means a **living human being** as distinguished from a legal person or entity; • Does not cover items specially designed for the surveillance of entities, objects, sites or machines.
"Monitoring, extracting, collecting, analyzing data"	• Implies that the items used for surveillance should have **precise technical capabilities** for the processing of data to monitor, collect, extract or analyze data; • Does not cover items that are not specially designed for monitoring, extracting, collecting and analyzing data and have to work with other technologies.
"From information and telecommunication systems"	• Refers to **systems** (and not equipment) which electronically **process information**, and to some systems which **convey information** over a distance.

The Guidelines also provide examples of **products and technology with potential for surveillance that warrant particular vigilance** from EU exporters. Those include facial and emotion recognition technology, location tracking devices and video-surveillance systems. Conversely, and consistent with Recital 8 of the Dual-Use Regulation, **items used for purely commercial applications** (*e.g.,* billing, marketing, quality services, user satisfaction or network security) are generally considered not subject to controls under Article 5.

Clarification of Scope of Obligation to Notify NCA of Potential Misuse of Non-Listed Cyber-Surveillance Items

EU exporters are required to notify their respective NCAs when they are "aware" that the Non-Listed Cyber-Surveillance Items may be "intended for" "internal repression" or "serious violations of human rights and international humanitarian law". These terms are not defined in the Dual-Use Regulation, and the new Guidelines fill this gap by providing the following definitions:

Term	Guidelines' Definition
"Aware"	• Means having a **positive knowledge of the intended misuse** of the cyber-surveillance items; • The mere possibility of such a risk is not sufficient to establish awareness, but EU exporters are **required to take steps** to (i) obtain sufficient and adequate knowledge for assessing the risks and (i) to ensure compliance with the Dual-Use Regulation.
"Intended for"	• Requires a case-by-case assessment, in light of the specific circumstances of the export; • A theorical risk of misuses of the items is not sufficient.

The Guidelines generally provide that the references to, "internal repression" or the commission of "serious violations of human rights and international humanitarian law", should be construed consistent with the definition of those terms in the EU Council Common Position 944/2008, its User Guide and the Guidelines of the International Committee of the Red Cross ("**ICRC**").

- Under the EU Common Position, internal repression notably covers "*torture and other cruel, inhuman and degrading treatment or punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.*" The User Guide provides guidance on the assessment criteria which may include the **end-user and destination country's current and past record with regard to respect for human rights**.
- Under the User Guide, **human rights violations** are considered "**serious**" when the **nature** and the **consequence** of the violation are **determinative**, which may include systematic and widespread violations.
- Under the ICRC Guidelines, **violations** of **international humanitarian law** are considered "**serious**" if they endanger **protected persons** (including civilians, prisoners of war, the wounded and sick) or **objects** (including civilian objects or infrastructure) or if they **breach** important **universal values**.

On the other hand, the Guidelines do not provide any details regarding the notification procedure to the NCAs in case of awareness of potential misuse of *Non-Listed Cyber-Surveillance Items*. In particular, it remains unclear what information should be provided to the NCA, and if so the deadline for providing such information.

New Step-by-Step Approach for Conducting Due Diligence in Connection with Non-Listed Cyber-Surveillance Items

To comply with their notification requirement, EU exporters must carry out due diligence on individual transactions (*i.e.,* transaction screening) that may involve Non-Listed Cyber-Surveillance Items. The Dual-Use Regulation does not describe the extent and content of the due diligence measures required in connection with exports of Non-

Listed Cyber-Surveillance Items, and the Guidelines contain a practical four-step approach to the due diligence to be undertaken by EU exporters summarized in the table below.

Importantly, EU exporters can also rely on existing guidance included in the Commission's recommendations on dual-use internal compliance programs ("**ICPs**") when conducting the assessment of potential risks of misuse of Non-Listed Cyber-Surveillance Items. Indeed, the Commission has in the past published two comprehensive sets of recommendations: (i) the 2019 general ICPs for dual-use trade controls and (ii) the 2021 ICPs on controls of research involving dual-use items, under the Dual-Use Regulation. Both sets of recommendations provide additional guidelines regarding "transaction screening process and procedures" that might help exporters of Non-Listed Cyber-Surveillance Items.

Step 1: Is the Non-Listed Item a Cyber-Surveillance Item as Defined in Article 5 of the Dual-Use Regulation?

• This consists of an examination of the **technical characteristics** of the item, on the basis of:
  o The technical parameters of cyber-surveillance items listed in Annex I to the Dual-Use Regulation*; or
  o The definition of Non-Listed Cyber-Surveillance Items.
**An Appendix to the Guidelines provides information on the technical parameters of listed cyber-surveillance items.*

Step 2: Does the Item Have the Potential for Misuse as part of Internal Repression or Serious Violations of Human Rights or International Humanitarian Law?

• Assessment of the potential for the item to be misused alone or as part or component of another system or item, **using red flags indicating inappropriate end-user, end-use or destination** such as:
  o Items marketed for potential covert surveillance;
  o Past misuse of similar items;
  o Items unlawfully used in surveillance activities directed against a Member State or in relation to unlawful surveillance on an EU citizen;
  o Items that could be used to set up, customize or configure a system known to be misused;
  o Items included in the lists published in the C series of the Official Journal of the EU in accordance with Article 5(6) of the Dual-Use Regulation.

Step 3: Do Stakeholders Involved in the Transaction Present Potential for Diversion and Misuse?

This includes the following:
 	
• **Review of end-use statements** to understand how the consignees and/or end-users (*e.g.,* distributors and resellers) intend to use the product or service both prior to and in the course of any transaction;
• Familiarization with the situation in the destination countr(ies) of the items, including the human rights situation;
• Review of **diversion risks** to different unauthorized end-users, based on **red flags** including *inter alia*:
  ○ Obvious relationship of end-user with a foreign government with a record of misuses;
  ○ End-user structurally part of the armed forces or another group involved in an armed conflict involving misuses in the past;
  ○ End-user previously exported cyber-surveillance items to countries where the use of such items has given rise to misuses.

Step 4: Prevent and Mitigate Potential Future Adverse Impacts

EU exporters are encouraged to:
 	
• Discontinue activities that cause or contribute to adverse impacts related to human rights; and
• Develop and implement a corrective action plan including *inter alia*:
  ○ Updating internal policies to provide guidance on how to avoid and address the adverse impacts in the future and ensure compliance therewith;
  ○ Updating and strengthening management systems to better track information and flag risks before adverse impacts occur;
  ○ Gathering information to understand high-level risks of adverse impacts related to the sector; and
  ○ Notifying the NCAs of the due diligence findings to facilitate information flow with regard to certain items, end-users and destinations.

Related People

Anne Hukkelaas Gaustad

Marie-Agnès Nicolas

Anita Maklakova

Aurore Maroteau

Lorenza Nava

Ilaria Bellini

Timothe Radosavljevic

Related Areas of Focus

Sanctions, Export Controls & Anti-Money Laundering