Official Journal
of the European Union

EN
L series

2024/2659

16.10.2024

COMMISSION RECOMMENDATION (EU) 2024/2659

of 11 October 2024

on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) Regulation (EU) 2021/821 of the European Parliament and of the Council ([1]) sets up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

(2) Regulation (EU) 2021/821 addresses the risk of cyber-surveillance items being used in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law.

(3) Pursuant to Articles 5(2) and 26(1) of Regulation (EU) 2021/821, the Commission and the Council shall make available guidelines for exporters with regard to non-listed cyber-surveillance items, in view of the need to ensure the efficiency of the Union export control regime as regards cyber-security and the consistency of the implementation of Regulation (EU) 2021/821.

(4) This Recommendation and the Guidelines attached thereto aim at supporting exporters in the application of controls on non-listed cyber-surveillance items, including, inter alia, due diligence measures assessing risks related to the export of such items.

(5) The Guidelines attached to this Recommendation were subject to extensive consultations in the Surveillance Technology Expert Group in 2022 and 2023 and took into account comments received during a public consultation ([2]) held in the second quarter of 2023.

(6) It should be recalled that this Recommendation, and the attached Guidelines, are non-binding. Exporters should therefore maintain the responsibility to comply with their obligations under Regulation (EU) 2021/821, while the Commission should ensure that this Recommendation remains relevant over time,

([1]) Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (OJ L 206, 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

HAS ADOPTED THIS RECOMMENDATION:

It is recommended that Member States' competent authorities and exporters take into account the Guidelines provided in the Annex to this Recommendation in order to fulfil their obligations under Article 5(2) of Regulation (EU) 2021/821.

Done at Brussels, 11 October 2024.

For the Commission
Valdis DOMBROVSKIS
Executive Vice-President

ANNEX

CONTENTS

INTRODUCTION

The Union Export Control Framework established by Regulation (EU) 2021/821 ('the Regulation') aims to ensure that the international obligations and commitments of the Union and its Member States, including regarding regional peace, security and stability and respect for human rights and international humanitarian law, are complied with. The Union and its Member States have therefore implemented the decisions made in the multilateral export control regimes and updated the Union control List in Annex I to the Regulation accordingly ([1]). Furthermore, before Article 5 of the Regulation was applicable, the competent authorities of the Member States had already controlled the export of certain listed items that may have surveillance applications ([2]), taking into consideration risks of misuse in certain specific circumstances. In the case of exceptionally grave circumstances, the Union has imposed sanctions restricting the export of certain surveillance equipment ([3]).

The Regulation reflects the Union's commitment to effectively address the risk of cyber-surveillance items being used in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law. The Regulation in particular introduces new provisions for the control of exports of non-listed cyber-surveillance items, including an obligation for exporters to notify the competent authority when they are aware according to their due diligence findings that non-listed cyber-surveillance items which the exporters propose to export, are intended, in their entirety or in part for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law. The Regulation further calls on the Commission and the Council to make available guidelines for exporters to support the effective implementation of the new controls for non-listed cyber-surveillance items.

These guidelines, therefore, aim at supporting exporters in the application of controls on non-listed cyber-surveillance items including, among others, due diligence measures assessing risks related to the export of such items to end-users and end-uses under the new provisions of the Regulation.

1. RELEVANT LEGAL PROVISIONS, DEFINITIONS AND KEY CONCEPTS

1.1. Overview of relevant legal provisions

The Regulation introduces new provisions specifically providing for controls on exports of cyber-surveillance items not listed in Annex I to the Regulation, that are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law. The relevant recitals and articles are:

(a) recital (8): 'In order to address the risk that certain non-listed cyber-surveillance items exported from the customs territory of the Union might be misused by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law, it is appropriate to place the export of such items under control. Associated risks relate, in particular, to cases where cyber-surveillance items are specially designed to enable intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert

([1]) See in particular controls relating to telecommunication interception systems (5A001.f), internet surveillance systems (5A001.j.), intrusion software (4A005, 4D004 and related controls under 4E001.a and 4E001.c) and law enforcement monitoring software (5D001.e). Furthermore see, based on a case-by-case assessment, controls relating to certain forensic/investigative tools (5A004.b 5D002.a.3.b and 5D002.c.3.b).

([2]) In particular Information Security systems.

([3]) See Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine (OJ L 134, 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (OJ L 100, 14.4.2011, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Council Regulation (EU) No 36/2012 of 18 January 2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011 (OJ L 16, 19.1.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Council Regulation (EU) No 401/2013 of 2 May 2013 concerning restrictive measures in view of the situation in Myanmar/Burma and repealing Regulation (EC) No 194/2008 (OJ L 121, 3.5.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); and Council Regulation (EU) 2017/2063 of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela (OJ L 295, 14.11.2017, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from those systems. Items used for purely commercial applications such as billing, marketing, quality services, user satisfaction or network security are generally considered not to entail such risks';

(b) recital (9): 'With a view to strengthening the effective control of exports of non-listed cyber-surveillance items, it is essential to further harmonise the application of catch-all controls in that area. To that end, Member States are committed to supporting such controls by sharing information amongst themselves and with the Commission, in particular regarding technological developments of cyber-surveillance items, and by exercising vigilance in the application of such controls to promote an exchange at Union level';

(c) Article 2, point (20), which provides for a definition of cyber-surveillance items as 'dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems';

(d) Article 5 introduces an authorisation requirement for the export of non-listed cyber-surveillance items if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law (Article 5(1)). It further requires exporters to notify the competent authority where they are aware, according to their due diligence findings, that the items are intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law (Article 5(2)). That competent authority is to decide whether to make the export concerned subject to authorisation; and

(e) Article 5(2) further stipulates that 'The Commission and the Council shall make available guidelines for exporters, as referred to in Article 26(1).'

1.2. **Key definitions**

The Regulation contains dedicated recitals and provisions that clarify specific terms relevant for controls on exports of non-listed cyber-surveillance items, and which are important for exporters to understand clearly in order to conduct due diligence and to implement controls effectively. Of particular relevance, Article 2, point (20), provides the following precise definition of 'cyber-surveillance items': '*dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems*'.

For the purposes of these guidelines, specific aspects of that definition should be clarified.

1.2.1. '*Specially designed*'

An item is designed for covert surveillance when its technical features are suitable for and objectively enable covert surveillance of natural persons. Therefore, the term 'specially designed' means that the covert surveillance of natural persons must have been the main purpose of the development and design of the product. However, such term does not require that the item can solely be used for the covert surveillance of natural persons.

As clarified in recital (8) of the Regulation, items used for purely commercial applications, such as billing, marketing, quality services, user satisfaction or network security, are not specially designed for covert surveillance of natural persons and thus do not fall under the definition of cyber-surveillance items. For example, even though items for the surveillance of operating systems in industry or the monitoring of users' traffic might be used for surveillance purposes, those items are not cyber-surveillance items under the definition since they are not specially designed to enable covert surveillance of natural persons.

1.2.2. *'Covert surveillance'*

Items enable covert surveillance in particular where surveillance is not obviously perceptible to the affected natural person. This would be the case when the concerned persons are not aware of the presence and/or action of cyber-surveillance items and hence do not have the opportunity to remove themselves from that surveillance or at least to adjust their behaviour accordingly. Even if the surveillance is conducted by means of items installed or operating in the public space, the acquisition of data can in certain cases be deemed as relevant to covert surveillance, notably the gathered data can be diverted, evaluated or processed for other purposes than the ones the affected natural person is made aware of. In other words, when a natural person cannot objectively expect to be under surveillance, the surveillance can be regarded as being covert according to Article 2, point (20), of the Regulation.

1.2.3. *'Natural persons'*

The term 'natural person' refers to a living human being by opposition to a legal person or entity, that are therefore not subject to the provisions. The term does not cover the surveillance of objects, sites or machines as such.

1.2.4. *'Monitoring, extracting, collecting, analysing data'*

According to the Oxford English Dictionary, the words monitoring, extracting, collecting and analysing have the following linguistic meaning:

— 'monitoring': overseeing; surveillance, listening in;

— 'extracting': to draw out;

— 'collecting': to gather, get together;

— 'analysing': to differentiate or ascertain the elements of something (complex) in order to determine its structure or nature, and hence to explain or understand it; to examine closely and methodically for the purpose of interpretation; to subject to critical or computational analysis.

These terms imply that the items used for surveillance should have precise technical capabilities for the processing of data in order to monitor, collect, extract or analyse data, such as, for example, the following items:

(a) Items used to monitor data from information and telecommunication systems ([4]) (for example, file size or package traffic of the data that are transmitted in such system);

(b) Items that extract data from information and telecommunications systems by performing intrusion and extraction (for example, intrusion software);

(c) Items that enable an analysis of data extracted from information and telecommunications systems, including those that can process camera images stocked in those systems (for example, certain types of data analysis technologies used as part of facial recognition systems).

Items used to simply monitor information systems or to watch the population via video surveillance cameras and that make it possible to capture conversations, data exchanges, movements and individual behaviours, would not be cyber-surveillance items within the definition of the Regulation as they are not specially designed for this purpose and have to work with other technologies, such as Artificial Intelligence or big data. However, the entire system (working together with other technologies like Artificial Intelligence or big data technologies) could potentially be a cyber-surveillance item under the definition of Article 2, point (20), of the Regulation.

Importantly, while providing some examples useful for illustration purposes, the definition and the scope of cyber-surveillance items is not limited by those examples, since the objective of Article 5 is to enable effective export control on non-listed items.

([4]) Please see 1.2.5. below for the definition.

As evidenced by the use of the conjunction 'or' in the definition, the listed technical capabilities are to be considered as alternatives, and it is not necessary for an item to have all those technical capabilities for monitoring, extracting, collecting or analysing data. In other words, it is sufficient for an item to have one of those technical capabilities to fall under the definition of cyber-surveillance item of Article 2, point (20).

1.2.5. *'From information and telecommunication systems'*

These terms refer to systems which electronically process information for example programming/coding, PC system (hardware) operations, and other information administration, including software technology, web technology, computer technology, storage technology, etc., and to some systems which convey information over a distance, for example technical systems transmitting sounds, signals, text, other signs, images through both wired and wireless channels, via optical fibres, radio and other electromagnetic system. Together, these two concepts include a broad range of systems transmitting or processing information. It should be noted that the term refers to systems and not equipment.

1.2.6. *'Awareness' and 'are intended for'*

Pursuant to Article 5(2) of the Regulation, an exporter is to notify the competent authority where the exporter is *'aware that cyber-surveillance items (…) are intended (…) for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law'*.

The term 'aware' is not a new legal concept but has been used in connection with end-use related authorisation requirements (so-called 'catch-all' controls) under Articles 4, 6, 7 and 8 of the Regulation. Being 'aware' implies that the exporter has positive knowledge of the intended misuse. The mere possibility of such a risk is not sufficient to establish awareness. The term 'awareness' however cannot be assimilated to passivity: it requires that the exporter has taken steps to obtain sufficient and adequate knowledge for assessing risks related to the export and to ensure compliance with the Regulation.

The indication that the items must be 'intended for' a relevant sensitive end-use implies that the exporter should assess the end-use on a case-by-case basis, in light of the specific circumstances of that case. *A contrario*, a theoretical risk, that is to say, not based on a factual assessment of the case, that the items might be used in a manner that violates human rights would not be sufficient to imply that they 'are intended for' a specific misuse under Article 5.

1.3. **Internal repression, serious violations of human rights and international humanitarian law**

Pursuant to Article 15 of the Regulation, which sets out the considerations for the assessment of an authorisation, the Member States are to take into account all relevant considerations, including those covered by the Council Common Position 2008/944/CFSP ([5]).

Article 5 of the Regulation extends controls to the export of non-listed cyber-surveillance items in consideration of the risk of them being used in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law. Common Position 2008/944/CFSP and the User's Guide to this Common Position ([6]) provide useful guidance in this respect.

([5]) Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment (OJ L 335, 13.12.2008, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) See User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Internal repression*

Pursuant to Article 2(2) of the Common Position 2008/944/CFSP, *'internal repression includes, inter alia, 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 on Human Rights and the International Covenant on Civil and Political Rights'* (ICCPR). The User's Guide to the Common Position 2008/944/CFSP provides guidance on the elements to be taken into consideration in the exporter's assessment, including the *'current and past record of the proposed end-user with regard to respect for human rights and that of the recipient country in general'*.

1.3.2. *Commission of serious violation of human rights*

The misuse of non-listed cyber-surveillance items may negatively impact a broad spectrum of human rights, and directly interferes with the right to privacy and to data protection. Arbitrary or unlawful surveillance may also violate other human rights, such as the right to freedom of expression, association and assembly, freedom of thought, conscience and religion, as well as the right to equal treatment or prohibition of discrimination, and the right to free, equal and secret elections. In particular cases, the surveillance, including monitoring or collecting of information of the natural persons, such as human rights defenders, activists, political figures, vulnerable populations and journalists, may lead to intimidation, suppression, arbitrary detention, torture or even extrajudicial killings. Therefore, exporters should include these aspects relating to serious violations of human rights in their assessments.

International practice shows that any restrictions to human rights must be 'appropriate' and in conformity with the international human rights standards. In practice, this means that adequate safeguards are in place to ensure that restrictions are provided for by law and preserve the essence of the rights. Subject to the principle of proportionality, restrictions may be made only if they are necessary and genuinely serve a legitimate purpose – for example, national or public security, public order, the protection of public health, or the protection of rights and freedoms of others.

Cyber-surveillance items may include legitimate and regulated tools for law enforcement applications, such as for the prevention, investigation, detection or prosecution of criminal offences including in the field of counterterrorism, or the execution of criminal penalties. At the same time, cyber-surveillance items can also be misused to commit serious violations of human rights and international humanitarian law when exported to repressive regimes or private end-users and/or into conflict areas.

This calls for a case-by-case assessment of the circumstances of a case, including the application of relevant regulations in light of any reports of serious violations of human rights by the competent bodies of for example, the United Nations, the Union or the Council of Europe. A lead for the 'seriousness' of human rights violations may be drawn from the recognition of those violations in information published by the competent bodies of the United Nations, by the Union or by the Council of Europe. It is not an absolute necessity for such explicit recognition by those bodies, but it is a significant factor for the criteria to be fulfilled.

According to the terms in Article 5, the violation of human rights must be 'serious'. Useful guidance to categorise possible human rights violations as 'serious' can be found in the User's Guide to Common Position 2008/944/CFSP. According to that Guide, the nature and consequences of the violation are determinative. Systematic and/or widespread human rights violations are regularly viewed as serious; but also, violations that are not systematic or widespread may be considered 'serious' – for example, due to the severity of the intervention for the affected persons.

Annex II of the User's Guide to Common Position 2008/944/CFSP provides for a non-exhaustive list of the main international and regional human rights instruments, including the International Convention on Civil and Political Rights (ICCPR), the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the European Convention for Human Rights (the Convention) and the Charter of Fundamental Rights (the Charter), that can provide important guidance for the interpretation and application of the criteria in support of robust human rights assessments. These instruments and their respective additional protocols represent the main international norms and standards in the areas of human rights and fundamental freedoms.

1.3.3. *Commission of serious violation of international humanitarian law*

International humanitarian law (also called the 'Law of Geneva' or the 'Law of armed conflict') has been developed through a range of international treaties, most importantly the Hague Regulations, the Geneva Conventions and their two Additional Protocols of 1977, and identifies rules which, in times of armed conflict, serve to protect people who do not or no longer participate in hostilities (for example civilians and wounded, sick or captured combatants) and impose upon belligerent parties limitations in regard to the means and methods of warfare (Law of the Hague).

The use of non-listed cyber-surveillance items should comply with international humanitarian law when they are deployed as means and methods of warfare in the context of an armed conflict. In such circumstances, the risk of serious violations of international humanitarian law is a consideration under the Regulation and, as for the commission of serious violations of human rights, should be assessed in light of the intended end-use of the items in the specific case. The User's Guide to Common Position 2008/944/CFSP provides guidance on the elements to be taken into consideration, including the recipient's past and present record of respect for international humanitarian law, the recipient's intentions as expressed through formal commitments and the recipient's capacity to ensure that the equipment or technology transferred is used in a manner consistent with international humanitarian law and is not diverted or transferred to other destinations where it might be used for serious violations of this law.

Pursuant to Article 5, the violation of international humanitarian law must be 'serious'. Guidance can be found in the User's Guide to Common Position 2008/944/CFSP, acknowledging that 'isolated incidents of international humanitarian law violations are not necessarily indicative of the recipient country's attitude towards international humanitarian law', while 'where a certain pattern of violations can be discerned or the recipient country has not taken appropriate steps to punish violations, this should give cause for serious concern'. The International Committee of the Red Cross (ICRC) has provided guidelines in respect of the assessment of international humanitarian law violations for export control purposes. According to the ICRC, 'violations of international humanitarian law are serious if they endanger protected persons (for example, civilians, prisoners of war, the wounded and sick) or objects (for example, civilian objects or infrastructure) or if they breach important universal values'. War crimes, for example, constitute serious violations of international humanitarian law. The ICRC further mentions similar factors to be considered as the User's Guide to Common Position 2008/944/CFSP, including formal commitments to apply rules of international humanitarian law, appropriate measures ensuring accountability for international humanitarian law violations, international humanitarian law training for the military, and prohibition of recruiting children for armed forces.

2. **TECHNICAL SCOPE**

2.1. **Listed cyber-surveillance items**

The Appendix to these guidelines provides information on cyber-surveillance items listed in Annex I to the Regulation, to assist exporters in the identification of potential non-listed cyber-surveillance items.

2.2. **Potential non-listed cyber-surveillance items**

While it is by definition impossible to provide an exhaustive list of those products that may be controlled as 'non-listed items' under Article 5, the following items could have a potential for surveillance and may warrant particular vigilance under the Regulation.

As clarified in recital (8) of the Regulation, 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 Article 5. Many of these items have information security (cryptographic or even cryptanalytic) functionalities that meet the control parameters under Category 5 part 2 of the control text in Annex I to the Regulation. Security network equipment – including routers, switches or relays, where the information security functionality is limited to the tasks of 'Operations, Administration or Maintenance' implementing only published or commercial cryptographic standards – is also not captured by the definition of 'cyber-surveillance items', though exporters should remain vigilant in consideration of various reports of misuse of such items for human rights violations.

2.2.1. *Facial and emotion recognition technology*

Facial and emotion recognition technologies have multiple uses other than cyber-surveillance – for example, for identification or authentication – and would not automatically fall within the definition. However, in certain circumstances, facial and emotion recognition technologies may fall within the scope of Article 2, point (20), of the Regulation.

Facial and emotion recognition technologies that can be used to monitor or analyse stored video images, could fall within the scope of the definition of cyber-surveillance item. However, even if the abovementioned criteria are met, it has to be carefully examined whether the software is specially designed for covert surveillance.

2.2.2. *Location tracking devices*

Location-tracking devices allow tracking of the physical location of a device over time, and some location tracking technologies have been in use for some time by law enforcement and intelligence agencies. Their potential for targeted and mass surveillance has evolved considerably, as tracking technologies have become more advanced – including satellite-based location tracking, cell tower-based location tracking, Wi-Fi and Bluetooth transceivers – and as 'tracking devices' such as smartphones and other electronic devices (for example in-vehicle systems in cars) have become widespread.

Location-tracking devices are used by law enforcement and intelligence agencies for example to collect evidence in the course of an investigation or to track suspects, but also by companies for commercial purposes, for example reporting on aggregated movement patterns in shopping streets, tracking employees working off-site, or for location-based advertising.

2.2.3. *Video-surveillance systems*

In order to help exporters identify potential cyber-surveillance, it is also helpful to clarify what items would not be covered by the definition. In this sense, for instance, video-surveillance systems and cameras – including high-resolution cameras – used for the filming of people in public spaces are not covered by the definition of cyber-surveillance items, as they do not monitor or collect data from information and telecommunication systems.

3. **DUE DILIGENCE MEASURES**

According to Recital 7 of the Regulation, *'the contribution of exporters […] to the overall aim of trade controls is crucial. In order for them to be able to act in conformity with this Regulation, the assessment of risks related to transactions concerned by this Regulation is to be carried out through transaction-screening measures, also known as the due diligence principle, as a part of an Internal Compliance Programme (ICP)'.*

Article 2, point (21) defines an Internal Compliance Programme (ICP) as *'ongoing effective, appropriate and proportionate policies and procedures adopted by exporters to facilitate compliance with the provisions and objectives of this Regulation and with the terms and conditions of the authorisations implemented under this Regulation, including, inter alia, due diligence measures assessing risks related to the export of the items to end-users and end-uses'.*

Commission Recommendation (EU) 2019/1318 ([7]) provides a framework to help exporters identify, manage and mitigate risks associated with dual-use trade controls and to ensure compliance with the relevant Union and national laws and regulations.

These guidelines may support exporters when conducting transaction-screening measures, also known as the due diligence principle, as part of an ICP.

Pursuant to Article 5(2) of Regulation (EU) 2021/821, exporters of non-listed cyber-surveillance items are required to carry out due diligence through transaction-screening measures, meaning taking steps regarding item classification and transaction risk assessment. Practically, exporters are encouraged to review the following:

([7]) Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009 (OJ L 205, 5.8.2019, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Review if the non-listed item to be exported might be a 'cyber-surveillance item' that is to say specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems**

This step concerns the determination of the item under the provisions applying to cyber-surveillance items. This includes an examination of the technical characteristics of the items, on the basis of the technical parameters set out in Annex I to the Regulation for the listed items, and in light of the specific terms and concepts in the definition of cyber-surveillance items for non-listed items, and to the subsequent classification of the item (goods, technology or software).

3.2. **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**

Exporters should carry out an assessment to determine if the product could be misused to commit internal repression, violate or abuse human rights, including the right to life, freedom from torture, inhuman and degrading treatment, the right to privacy, right to freedom of speech, the right to association and assembly, the right to freedom of thought, conscience and religion, the right to equal treatment or prohibition of discrimination or the right to free, equal and secret elections.

It also includes an assessment to determine whether the product could be used as part or component of a system that could result in the same violations and/or misuse.

Exporters should use in their assessment so-called red flags which refer to any abnormal circumstances in a transaction that indicate that the export may be destined for an inappropriate end-use, end-user, or destination.

Red flags:

(a) the item is marketed with information in relation to its potential use for covert surveillance;

(b) information indicating that a similar item has been misused in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law (see section 1.3);

(c) information indicating that the item has been unlawfully used in surveillance activities directed against a Member State or in relation to unlawful surveillance on an EU citizen;

(d) information indicating that the transaction includes items that could be used to set up, customise or configure a system that is known to be misused in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law (see section 1.3);

(e) the item or a similar item is found on the list published in the C series of the *Official Journal of the European Union* in accordance with Article 5(6) of the Regulation.

3.3. **In support of competent authorities, review stakeholders involved in the transaction (including end-user and consignees such as distributors and resellers)**

Exporters should, in support of competent authorities, and to the extent possible:

(a) 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;

(b) familiarise themselves with the situation in the relevant destination of the items, especially with the general condition of human rights, as this provides an important indicator of the risk of serious violations of human rights and international humanitarian law connected with an export;

(c) review risks that the product or service will be diverted to a different unauthorised end-user, based on red flags as listed below.

Red flags:

(a) the end-user has an obvious relationship with a foreign government that has a record of committing internal repression and/or serious violations of human rights and international humanitarian law;

(b) the end-user is structurally part of the armed forces or another group involved in an armed conflict involving internal repression measures and/or serious violations of human rights and international humanitarian law in the past;

(c) the end-user has 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 of human rights and international humanitarian law.

3.4. Use the due diligence findings to draw up plans to prevent and mitigate potential future adverse impacts

Exporters should, based on their due diligence findings, discontinue activities that cause or contribute to adverse impacts related to human rights, as well as develop and implement a corrective action plan. Such actions may include:

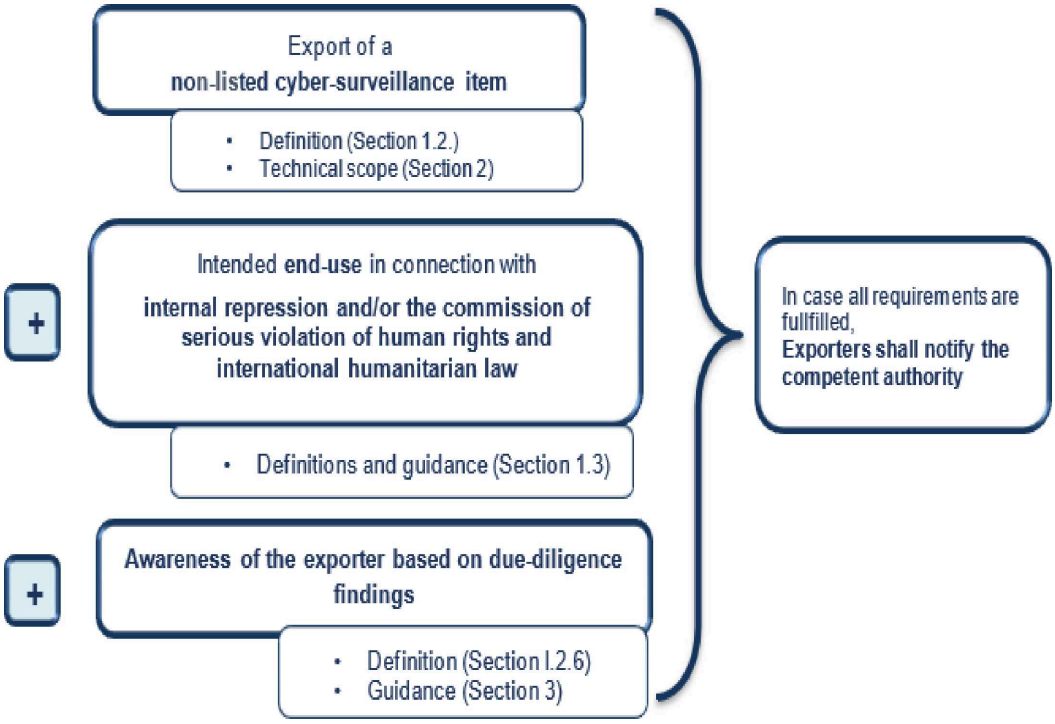
(a) update the enterprise's policies to provide guidance on how to avoid and address the adverse impacts in the future and ensure their implementation;

(b) draw from the findings of the risk assessment to update and strengthen management systems to better track information and flag risks before adverse impacts occur;

(c) gather information to understand high-level risks of adverse impacts related to the sector;

(d) notify the competent authorities of the Member States of the due diligence findings to facilitate information flow with regards to certain items, end-users and destinations.

Requirements set out by Article 5(2) of Regulation (EU) 2021/821



4. APPENDIX

Listed cyber-surveillance items as controlled by Annex I to Regulation (EU) 2021/821

— **Telecommunication interception systems (5A001.f.)**

In most countries, including Member States, the confidentiality of communications is protected by law, but the covert electronic surveillance of communication by government authorities may be authorised within a legal framework (so-called Lawful Interception (LI)). The digital era however ushered in the possibility for using interception technologies on a mass scale. The use of interception tools by the Libyan regime highlighted the potential to deploy these technologies on a mass scale and spurred the introduction of export controls on telecommunication interception systems in 2012.

This control applies to equipment designed for the extraction of the content of a communication (voice or data), as well as subscriber identifiers or other metadata that is transmitted over the air via wireless communication, and radiofrequency monitoring equipment. This control applies for example to IMSI-catchers (International Mobile Subscriber Identity) that intercepts mobile phone traffic and tracks the movement of mobile phone users or to equipment creating fake Wi-Fi hotspots that can extract IMSI numbers from a telephone, as well as to certain types of items specially designed to enable 'deep packet inspection' into telecommunications systems. Mobile telecommunications jamming equipment does not fall within the scope of cyber-surveillance items, as it does not collect data.

While general-purpose technology can be used to build such systems, their capabilities of interception on a mass scale will rely on specific parts and components, including for example specific software, advanced or application-specific integrated circuits (for example FPGAs, ASICs, etc.) to boost the number of packets or communication sessions that can be processed per second.

— **Internet surveillance systems (5A001.j.)**

Although many internet-based communication is now typically encrypted by default, interception of traffic data (metadata) about communications – such as IP addresses and frequency and sizes of data exchange – can still be used to identify links between persons and domain names. Governments may use these systems lawfully, and with judicial oversight, for legitimate purposes, such as identifying persons who visit domains associated with criminal or terrorist content. The monitoring and analysis of internet traffic on the basis of ethnical, religious, political or social characterisation can however lead to a comprehensive human and social mapping of a country for population control and repression, as well as other purposes, for example to identify political dissidents. In addition to issues concerning human rights and internal repression, these items can also contribute to the enhancement of the security and military capabilities.

The control under 5A001.j applies to internet control systems that operate on a 'carrier class IP network (for example, national grade IP backbone)' to perform analysis, extraction and indexing of transmitted metadata content (voice, video, messages, attachments) on the basis of 'hard selectors', and map the relational network of people. These are items which perform 'covert surveillance' because the targeted persons are not aware of the communications interception. By contrast, controls do not aim at systems where an action of, or an interaction with, a user or a subscriber, exists and for example, do not apply to social networks or commercial search engines. Moreover, controls apply to systems that process data coming from an internet provider core network, and do not apply to social networks or commercial search engines which process data given by users.

— **'Intrusion software' (4A005, 4D004 and related controls under 4E001.a. and 4E001.c.)**

Intrusion software allows its operator to covertly obtain remote access to an electronic device, such as a smartphone, laptop, server or an internet of Things device, to obtain data stored on the device, to eavesdrop via a camera or microphone built in or connected to the device, and to use the device as a stepping stone to carry out attacks on equipment to which the device connects, or against contacts of the user ('hacking via third-party devices'). While there are legitimate uses ([8]) of intrusion software for example, 'remote access software' used for remote support from IT departments, the covert nature of the surveillance and the magnitude of information possibly collected, presents a high risk of violation of the right to privacy and personal data protection, and may seriously undermine the right to freedom of expression.

([8]) For the sake of clarity, listed cyber-surveillance items as controlled by Annex I to the Dual-Use Regulation would need an authorisation to be exported to third countries, regardless if the use of the item is legitimate.

The control under 4A005 et al includes software as well as systems, equipment, components, and related technology, specially designed or modified for the generation, command and control, or delivery of 'intrusion software', but does not apply to 'intrusion software' itself, as defined in Annex I to the Regulation. These cyber tools are controlled in consideration of the potential disruption and damage they can cause if utilised and executed successfully but controls are not meant to affect the activity of the cyber security researchers and industry for example, as they need to share information related to intrusion software in order to be able to develop fixes for their products and have them in place prior to the public release of a vulnerability.

— **Communication monitoring software (5D001.e.)**

This software is designed for monitoring and analysis by authorised law enforcement authorities of data collected through targeted interception measures requested from a communications service provider. This software allows for searches based on 'hard selectors' of communication content or metadata, using an interface for lawful interception, and mapping the relational network or tracking the movement of targeted individuals based on the results of searches. This software is intended for 'covert surveillance' because it uses data collected from the interception of communications without persons being aware of it. It furthermore 'analyses' data collected via 'telecommunications systems'. The software is installed in the governmental authority (for example, law enforcement monitoring facility (LEMF)), and the control does not apply to the lawful interception (LI) compliance systems (for example, LI management systems and mediation devices) that are commercially developed and installed in the communications service provider's space (for example, integrated into the communications network), and that the service provider operates and maintains. As clarified in the control text, controls do not apply to 'software' specially designed or modified for purely commercial purposes such as billing Network Quality of Service (QoS), Quality of Experience (QoE), mediation devices or mobile payment or banking use.

— **Items used to perform cryptanalysis (5A004.a.)**

This control applies to items designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys. Cryptography is used to safeguard the confidentiality of information in transit and at rest. Cryptanalysis is used to defeat this confidentiality, and this technology therefore 'enables' covert surveillance by monitoring, extracting, collecting, or analysing data from information and telecommunication systems.

— **Forensic/investigative tools (5A004.b., 5D002.a.3.b. and 5D002.c.3.b.)**

Forensic/investigative tools are designed to extract raw data from a device (for example, computing or communication) so that the data is not tampered with or corrupted and can be used for judicial purposes, i.e., in a criminal investigation or court of law. These products circumvent 'authentication' or authorisation controls of a device so that the raw data can be extracted from the device. These products are used by government and law enforcement agencies, but also by military forces to extract and analyse data from seized devices. While they have legitimate uses, they can however be misused and thus pose a risk for sensitive or commercial data.

However, forensic/investigative tools that are not 'specially designed' for covert surveillance do not fall under the definition of cyber-surveillance items of Article 2, point (20). Also, forensic/investigative tools which only extract user data or where the data is unprotected on the device are not captured by the control text in 5A004.b. et al. At the same time, controls do not apply to manufacturer's production or testing equipment, system administrator tools or products exclusively for the commercial retail sector for example mobile phone unlocking products. Therefore, considering that the variety of these types of technology, the application of controls depends on a case-by-case assessment of each product.

Finally, please note that there are other surveillance-related items listed in Annex I to the Regulation that should not be considered to fall within the definition of cyber-surveillance items, such as Mobile telecommunications jamming equipment (5A001.f.) designed for damaging or disrupting communications or systems, intrusion software which modifies a system (4D004), and laser acoustic detection equipment (6A005.g.) collecting audio data with a laser, or allowing for listening to conversations at a distance (sometimes called a 'laser microphone'). Similarly, the use of listed UAVs for surveillance purposes would not bring those items under the definition of cyber-surveillance items.