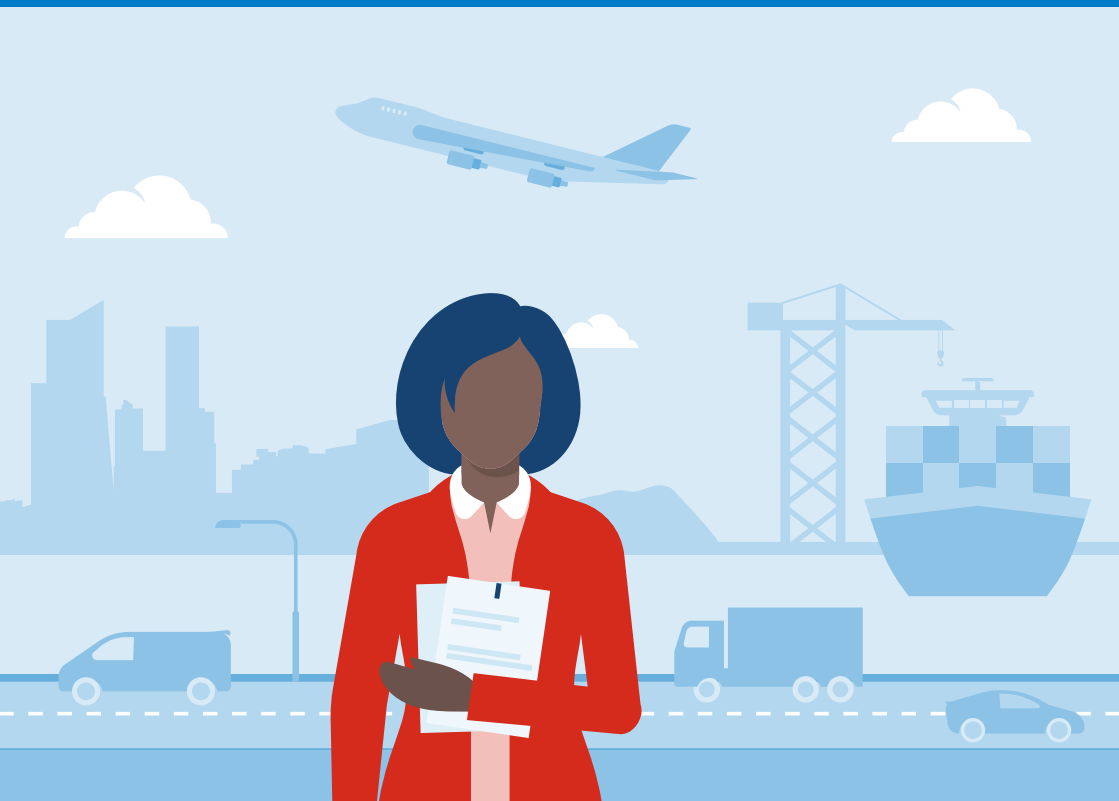




Ministry of Foreign Affairs

Export controls for cyber-surveillance items: A focus on protecting human rights

National policy framework pursuant to Article 5 of
EU Regulation 2021/821



Contents

	Introduction	3
1	An explanation of Dutch export control policy	4
2	Cyber-surveillance items	6
	<i>Scenario 1: Informing exporters of the authorisation requirement</i>	7
	<i>Scenario 2: Exporters' requirement to notify the competent authority</i>	8
	<i>Scenario 3: Authorisation requirement based on national legislation</i>	8
3	Guide for exporters for Scenario 2	9
4	Due diligence	18
	Contact	20



Introduction



With the entry into force of Regulation (EU) 2021/821¹ ('Dual-Use Regulation'), the protection of human rights has come to play a more central role in export control policy. This Regulation makes export controls on dual-use items in the EU a key instrument, especially with regard to the observance of international obligations and responsibilities related to the protection of human rights.

Protecting and promoting human rights, democracy, the rule of law and the international legal order lie at the heart of the Netherlands' foreign policy.

The more central role that the issue of human rights has come to play in the realm of export controls is evident from the decision to expand these controls to explicitly include cyber-surveillance items. If there are concerns about human rights violations, the Dual-Use Regulation makes it possible to subject such items, including software and technology, to ad hoc export controls.

In addition, the Regulation refers to companies' responsibility to practise responsible business conduct (RBC). Under the new provisions on cyber-surveillance items, companies are required to notify the national authority of any risks of human rights violations their due diligence may have identified.

This policy framework aims to inform exporters, knowledge institutions and government agencies about how this new legislation will be implemented and applied. It deals with the requirements arising from Article 5 of the Dual-Use Regulation, with a particular focus on the obligations it entails for exporters.

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

Companies or persons wishing to export items that are listed in Annex I of the Dual-Use Regulation must apply to the Central Import and Export Office (CDIU) for a licence, referred to as an export authorisation.

The CDIU, which is a subdivision of the Customs Administration, is responsible for issuing export authorisations under the policy supervision of the Ministry of Foreign Affairs (MFA). Certain applications (often those of a sensitive nature) are forwarded to the Ministry of Foreign Affairs for a decision. Authorisations are issued on behalf of the Minister for Foreign Trade and Development.

Dutch export control policy seeks to ensure that the export of dual-use items, whether directly or indirectly (due to forwarding), does not lead to any of the following undesirable consequences:



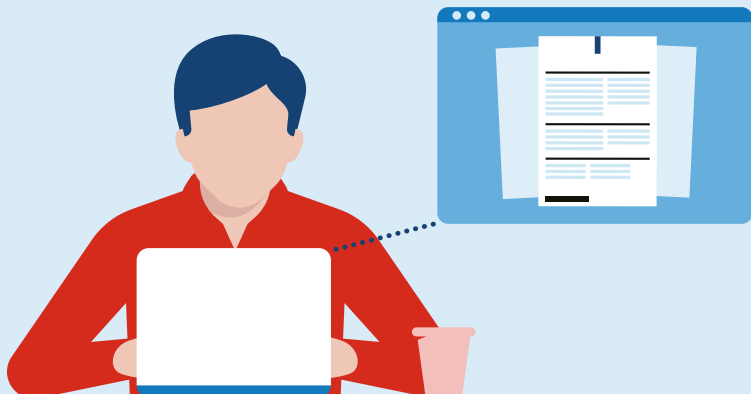
the development or proliferation of weapons of mass destruction or their means of delivery;



contributing to human rights violations, internal repression, international aggression or regional instability;



conventional military use in conflict zones or use for terrorist purposes.



In order to gauge the risk of these undesirable consequences occurring, we assess authorisation applications for dual-use items on the basis of the following factors:



Exporter



Nature of the good or service



Stated end use



Potential undesirable end use



Recipient and end user

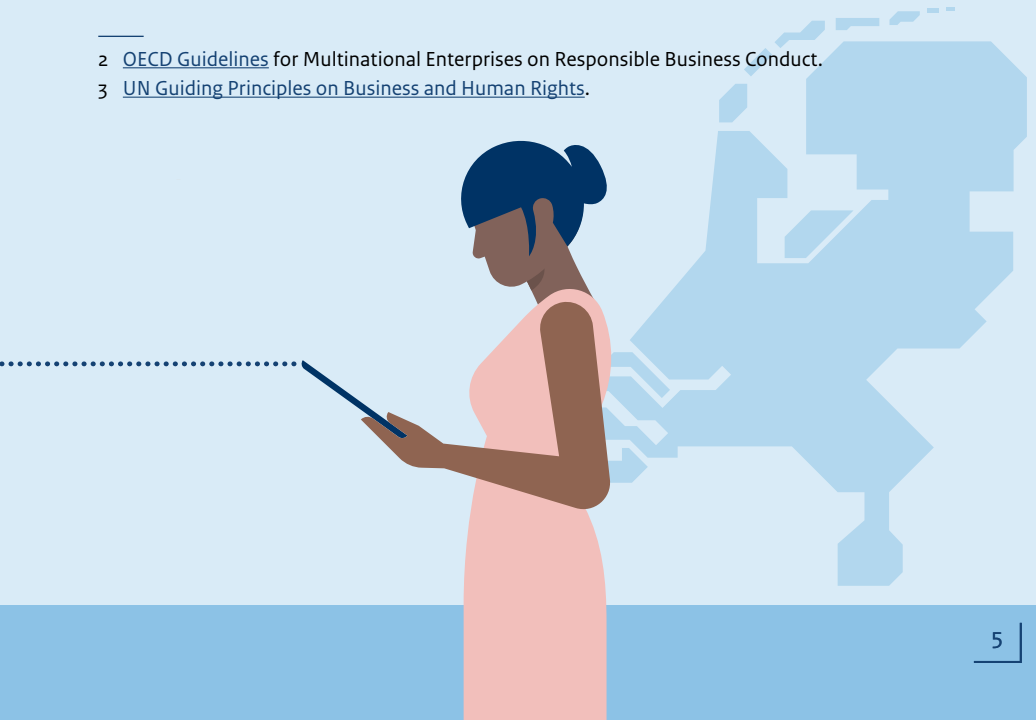


Country of destination

In assessing authorisation applications for dual-use items, including software and technology, we explicitly consider the risk of human rights violations. If there are concerns about the end use or end user in relation to human rights violations, the application will be denied. In addition, Dutch companies are expected to practise due diligence as described in the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct² and the UN Guiding Principles on Business and Human Rights.³

² [OECD Guidelines](#) for Multinational Enterprises on Responsible Business Conduct.

³ [UN Guiding Principles on Business and Human Rights](#).



2 Cyber-surveillance items

Since 1 September 2021 the Dual-Use Regulation has *explicitly* classified cyber-surveillance items as dual-use items within the meaning of Article 2.

Article 2(20) defines ‘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** [emphasis added]’.



What the Dual-Use Regulation says about cyber-surveillance items

According to consideration (8)⁴ of the Dual-Use Regulation, it is appropriate to place the export of such items under control in order to address the risk that certain cyber-surveillance items – not listed in Annex I – 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.

Consideration (8) further states that the risks associated with the export of such cyber-surveillance items relate, in particular, to ‘cases where these items are specially designed to enable intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from those systems.

Items used for *purely* [italics added] commercial applications such as billing, marketing, quality services, user satisfaction or network security are generally considered not to entail such risks.’

⁴ Page 2, Consideration (8), Regulation (EU) 2021/821

The new provision on cyber-surveillance makes it possible to impose an **ad hoc authorisation requirement** for cyber-surveillance items under Article 5. Article 5 lists three scenarios in which this ad hoc authorisation requirement can be imposed. Below we explain the difference between them. The scenarios have in common that the authorisation requirement is based on **human rights requirements**.

An ad hoc authorisation requirement means that the government can impose an authorisation requirement on an exporter for items that would not otherwise require one. In other words, items not listed in Annex I of the Dual-Use Regulation. If an ad hoc authorisation requirement is imposed on an exporter, they will be informed accordingly by the CDIU or the MFA by way of a formal decision.

Scenario 1: Informing exporters of the authorisation requirement

Under Article 5(1), the CDIU and the MFA will impose an authorisation requirement on exporters of cyber-surveillance items (which are not listed in Annex I), if they deem it possible that these items are or may be intended, in their entirety or in part, for use in connection with sensitive end use within the meaning of this paragraph.



Article 5(1)

‘An authorisation shall be required for the export of cyber-surveillance items not listed in Annex I 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.’

Scenario 2: Exporters' requirement to notify the competent authority

On the basis of the results of their due diligence, the exporter is obliged to notify the CDIU.



Article 5(2)

'Where an exporter is aware, according to its due diligence findings, that cyber-surveillance items which the exporter proposes to export, not listed in Annex I, are intended, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article, the exporter shall notify the competent authority. That competent authority shall decide whether or not to make the export concerned subject to authorisation. The Commission and the Council shall make available guidelines for exporters, as referred to in Article 26(1).'⁵

⁵ [EU Guidelines on the Export of Cyber-Surveillance Items](#)

Scenario 3: Authorisation requirement based on national legislation

In certain circumstances member states can decide to introduce national legislation that imposes additional requirements for the export of cyber-surveillance items. This is not currently⁶ the case in the Netherlands.

⁶ Date of publication: January 2025.

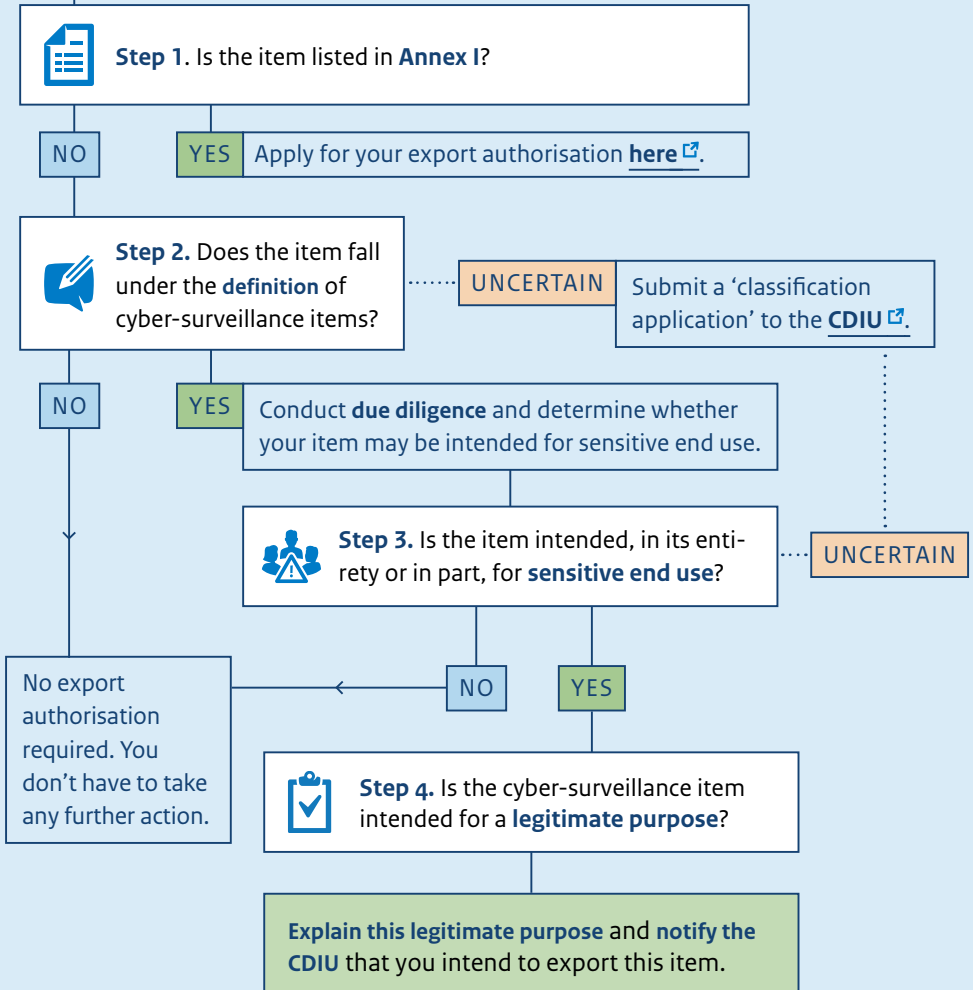


Article 5(3)

'A Member State may adopt or maintain national legislation imposing an authorisation requirement on the export of cyber-surveillance items not listed in Annex I if the exporter has grounds for suspecting that those items are or may be intended, in their entirety or in part, for any of the uses referred to in paragraph 1 of this Article.'

In practice, **Scenario 2** will be the most relevant situation for exporters. For that reason the rest of this policy framework deals with the requirements laid down in Article 5(2). They are explained with the help of a **four-step** flow chart and the pages that follow.

Do you need an export authorisation for your item?





Is the item listed in Annex I?

In order to meet the requirements of Article 5(2), it is necessary for the exporter to **first verify** whether the items are listed in Annex I of the Dual-Use Regulation.

NO

Are the items not on the list? Then the exporter should continue **to step 2**.

YES

Are the items on the list? Then the exporter must by definition apply for an export authorisation and the rest of this policy framework does not apply.





Does the item fall under the definition of cyber-surveillance items?

The definition of ‘cyber-surveillance item’, which is given in Article 2(20) of the Dual-Use Regulation, contains several elements that can be interpreted in various ways. Below is the Netherlands’ interpretation⁷ of these elements with regard to assessing whether a given item constitutes a cyber-surveillance item.

- **specially designed**

In the case of cyber-surveillance items this means that enabling the covert surveillance of natural persons must have been the *main purpose* of developing and designing the item. This does not mean that the item can *only* be used to conduct covert surveillance of natural persons, but rather that the design contains technical features/characteristics that enable the covert surveillance of natural persons. Thus, the design criterion⁸ plays a key role within the definition of cyber-surveillance items and should be assessed on a case-by-case basis. This criterion includes, for example, the *nature of the data collected* by means of a cyber-surveillance item.⁹

- **covert surveillance**

The surveillance of natural persons should be considered ‘covert’ when that surveillance *is not clearly observable*, but also when the person in question *has not been made aware of the purpose*¹⁰ of that surveillance.

- **from information and telecommunication systems**

These terms refer to a wide range of systems that either electronically *transmit* information (such as sounds, signals, text, images) or *process* it (in the form of programming/coding).

7 The interpretation of the qualification ‘specially designed’ is a national discretionary competence.

8 [The new rules for export control of cyber-surveillance items in the EU \(p.20\)](#).

9 [The new rules for export control of cyber-surveillance items in the EU \(par. 3.2.2\)](#) for a non-exhaustive list of possible criteria.

10 [The new rules for export control of cyber-surveillance items in the EU \(p.18\)](#).

- **monitoring, extracting, collecting or analysing**

These terms mean that the items used for surveillance must have precise technical capabilities for *collecting* and/or *processing* data (i.e. the use of the data after it has been gathered) on natural persons. The use of the word 'or' is meant to indicate that these capabilities should not be seen as cumulative. In other words, an item does not have to possess all these technical capabilities in order to meet the definition given in Article 2(20).

In addition, an exporter can examine the cyber-surveillance items listed in Annex 1 as a **guide** for the relevant features and technical characteristics. As stated in the section on the ad hoc authorisation requirement, Article 5 applies only to items not listed in Annex I. Although this policy framework does not apply to cyber-surveillance items that *are* on this list, these items can serve as a guide for identifying potential cyber-surveillance items.



Cyber-surveillance items listed in Annex I

- Mobile telecommunications interception or jamming **equipment**, and monitoring equipment therefor (5A001.f),
- Internet Protocol (IP) network communications **surveillance systems or equipment**, and specially designed components therefor (5A001.j),
- **Systems, equipment, and components, plus 'software' therefor**, specially designed or modified for the generation, command and control, or delivery of 'intrusion software' (4A005, 4D004 and related controls under 4E001.a and 4E001.c),
- **'Software'** specially designed or modified for monitoring or analysis by law enforcement (5D001.e),
- **Forensic/investigative tools** (5A004.b, 5D002.a.3.b and 5D002.c.3.b).

NO

The item does not fall under the definition of cyber-surveillance items. No export authorisation is required. The exporter doesn't have to take any further action.

YES

If the item falls under the definition of cyber-surveillance items within the meaning of Article 2(20), the next step is for the exporter to conduct their **due diligence**¹¹ and then to proceed to **step 3**. Under Article 5(2), exporters are required to notify the competent national authority of risks of human rights violations their due diligence may have identified.

Article 5(2) contains multiple elements that can be interpreted in various ways. The Netherlands' interpretation is explained below, so you can determine whether you need to notify the CDIU.

- **'is aware'**

The term 'aware' means that the exporter has positive knowledge of any *sensitive end use*. A mere belief in the possibility of such a risk does not constitute 'awareness'. There must be a considerable degree of probability. However, the 'awareness' in question should not be passive in form: it requires the exporter to take *steps* to ensure they have sufficient knowledge *that can be used* to assess the risks associated with the export and to guarantee observance of the Regulation.

- **'intended for'**

When the passage refers to an item 'intended for' sensitive end use, this means that the exporter must determine the specific purpose of the end use on a case-by-case basis, in light of the factual circumstances. The existence of a mere 'theoretical risk' is not enough to imply that the items are 'intended for' any of the uses referred to in Article 5(1). This differs from Article 5(1) itself, where it is sufficient that the items 'may be' intended for any of the uses referred to in that paragraph.

UNCERTAIN

If an exporter remains in doubt, they can submit a classification application to the CDIU, using this form¹² from the Customs Administration.

¹¹ [EU Guidelines on the export of cyber-surveillance items](#)

¹² Classification application ([belastingdienst.nl](#)).



Is the item intended for sensitive end use?

If **due diligence** (see p. 18) reveals that the item is intended, in its entirety or in part, for *sensitive end use*, i.e. any of the uses referred to in Article 5(1), the exporter is required to notify the CDIU. The exporter must use their due diligence findings to determine whether the cyber-surveillance item is intended for a *legitimate end use* and whether *mitigating measures* can be taken to prevent *misuse*.

‘Sensitive end use’ means that the item is or may be intended, in its entirety or in part, for use in connection with:

a. Internal repression

According to Article 2(2) of Common Position 2008/944/CFSP of the Council: ‘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 Rights¹³ and the International Covenant on Civil and Political Rights.’¹⁴

b. Serious violations of human rights

The *misuse* of cyber-surveillance items that are not listed in Annex I can have a negative impact on a wide range of human rights. The following rights are in particular danger of being violated through the use of cyber-surveillance items: the right to privacy and to the protection of data, the right to freedom of expression, association and assembly, the right to freedom of thought, conscience and religion, the right to equal treatment or the prohibition of discrimination, and the right to free and fair elections by secret ballot. In certain cases the monitoring of human rights defenders and journalists can lead to random detention, torture or even extrajudicial executions. Restrictions on the above-mentioned rights must be ‘*appropriate*’ and in accordance with international human rights standards. In practice this means that the restrictions must be prescribed by law, must serve a *legitimate purpose* and must be proportional,

¹³ [Universal Declaration of Human Rights](#)

¹⁴ [International Covenant on Civil and Political Rights](#)

and that there must be *guarantees in place to prevent misuse*. A legitimate purpose might be national security or public safety, public order, or the protection of public health, public morals or the rights and freedoms of others. An indication that a given human rights violation is ‘serious’ can be inferred from the recognition of the violation in information published by the competent bodies of the UN, by the European Union or by the Council of Europe. It is not absolutely essential that such institutions explicitly refer to the violation, but it is a key factor for meeting these criteria.

c. Serious violations of international humanitarian law

International humanitarian law (in particular the Geneva Conventions) sets down rules for armed conflict, designed to protect people who are not involved (or who are no longer involved) in hostilities (e.g. civilians, the wounded, the sick or prisoners of war) and imposes restrictions on warring parties with regard to the means and methods of warfare used (the Hague Conventions). The use of cyber-surveillance items not listed in Annex I must be done in accordance with international humanitarian law if they are used as a means and method of war in the context of an armed conflict. In such circumstances the risk of serious violations of international humanitarian law is a consideration in the context of Article 5 and, as with the risk of human rights violations, *the specific purpose of the end use* must be assessed on a case-by-case basis.

NO

The item is not intended for sensitive end use. No export authorisation is required. The exporter does not have to take any further action.

YES

The item is intended for sensitive end use. The exporter continues to **step 4**.

UNCERTAIN

If an exporter remains in doubt, they can submit a classification application to the CDIU, using this form¹⁵ from the Customs Administration.

First and foremost, due diligence measures are meant to determine whether the cyber-surveillance items, in their entirety or in part, are intended for *sensitive end use* within the meaning of Article 5(1), and secondly, whether there is a *legitimate end use*. As stated in Article 5(1-3) the legitimacy of the trade in cyber-surveillance items depends on whether their intended *end use* respects *human rights*.

¹⁵ Classification application (belastingdienst.nl).



Is the cyber-surveillance item intended for a *legitimate purpose*?

If it has been determined that the cyber-surveillance items are intended for *sensitive end use*, the due diligence measures must establish that there is a *legitimate end use*.

This means that exporters must take *steps* with regard to *obtaining sufficient knowledge* about (1) *the item* and (2) the *legitimacy of a particular end use* by (3) *a particular end user*. In other words, it is necessary to gather enough knowledge that *can be used* to assess the transaction risk (see p. 18).

Explain this legitimate purpose and notify the CDIU that you intend to export this item.

On the basis of their **due diligence findings**, exporters have a duty to notify the CDIU of their intention to export the cyber-surveillance item. The exporter must use their due diligence findings to determine whether the cyber-surveillance item is intended for a *legitimate end use* and whether *mitigating measures* can be taken to prevent misuse.

The government will assess the application and decide if the *end use is legitimate*.

More information

[Central Import and Export Division \(CDIU\)](#)

[CDIU User Guide on Strategic Goods \(website in Dutch\)](#)

[Export guide | RVO.nl \(website in Dutch\)](#)

[OLEV: Export of Strategic Goods \(website in Dutch\)](#)

[National Contact Point for Knowledge Security](#)

[Export Control of Strategic Goods](#)

[Factsheets on Export Control of Strategic Goods \(website in Dutch\)](#)

[User Guide on Strategic Goods and Services](#)

[Dutch Export Control Policy in 2023 \(website in Dutch\)](#)

[Regulation \(EU\) 2021/821](#)

[Strategic Goods Order \(website in Dutch\)](#)

[Strategic Services Act \(website in Dutch\)](#)

[Exporting dual-use items - European Commission](#)

[Dual-use export controls | EUR-Lex](#)

[EU Sanctions Map](#)

[EU guidelines for the export of cyber-surveillance items](#)

[EU guidelines on establishing an internal compliance programme \(ICP\)](#)



According to the Dual-Use Regulation, exporters make a crucial contribution to the general goal of trade controls. In order to comply with the Regulation, they must assess the risks of their transactions via transaction screening, also known as the due diligence principle, as part of an internal compliance programme (ICP).

Recommendation (EU) 2019/1318 of the Commission provides a framework that is intended to help exporters to understand the impact of controls on the trade in dual-use items, and limit the risks. This recommendation, which applies to cyber-surveillance items not listed in Annex I, can help exporters carry out transaction screening.

1. Briefly put, **exporters** need to gather enough knowledge *that can be used* to assess the transaction risk.
2. **Exporters** must ensure that they are familiar with the cyber-surveillance items they export and with their possible applications.
3. **Exporters** must conduct an assessment to determine whether the items are intended for *sensitive end use* within the meaning of Article 5(1).
4. **Exporters** must familiarise themselves with the human rights situation in the country of the intended end user. A further key factor is the *specific goal* for which the end user intends to use the cyber-surveillance items, especially the *credibility* of the goal and the question of whether *mitigating measures* can be taken to prevent *misuse*.

Particular caution is necessary when cyber-surveillance items are supplied to foreign government bodies (police forces, agencies concerned with combating terrorism, cybercrime and drug crime, intelligence and security services, parts of the Ministry of Defence, research institutes and universities that are affiliated with the Ministry of Defence, border security and the coastguard) or to private end users that have close ties to government bodies.

Here, too, if exporters have doubts about the intentions of the end user, they can submit a classification application to the CDIU by means of the relevant form¹⁶ on the website of the Customs Administration.

In all cases Dutch companies are expected to practice due diligence in line with international standards on responsible business practices (OECD Guidelines and UN Guiding Principles).

This due diligence means that companies must prevent, limit or end the potential or actual effects of their activities on human rights and the environment to the greatest possible extent.

¹⁶ Classification application (belastingdienst.nl).



Contact

If you have any questions about the application of Article 5 of the Dual-Use Regulation, please contact the **Central Import and Export Division (CDIU)**, Postbus 3070, 6401 DN Heerlen.

Phone: +31 (0)88 151 2122

Email: cdiu@douane.nl



Publication information

Ministry of Foreign Affairs
Postbus 20061 | 2500 EB Den Haag

Phone: + 31 (0)70 348 6486

(Monday to Friday, 7.00 - 19.00)

© Ministry of Foreign Affairs | 2025

This brochure was prepared with the utmost care, ensuring that relevant sources were cited. In the interest of readability certain legal passages were simplified somewhat, including excerpts from legislative texts. No rights can be derived from this brochure or the examples it includes. The Ministry of Foreign Affairs is not liable for any consequences of its use.