SIPRI Good Practice Guide
March 2026

GOOD PRACTICE GUIDE ON APPLYING EXPORT CONTROLS TO TRANSFERS OF COMMERCIAL CYBER INTRUSION CAPABILITIES

MARK BROMLEY AND KOLJA BROCKMANN*

SUMMARY

● States supporting the Pall Mall Process (PMP) Code of Practice for States have committed to using export controls to help ensure accountability across the market for commercial cyber intrusion capabilities (CCICs) and to mitigate risks of potential irresponsible use of CCICs. Export controls can prevent transfers of CCICs that threaten human rights and national security by enabling the application of risk assessment frameworks to export licence applications, and can improve oversight of the international market for CCICs by enabling the sharing and publishing of export licence approvals and denials. However, the potential application of export controls to the transfer of CCICs is limited by the complexities associated with their establishment, implementation and enforcement, and a lack of guidance to inform national practices. This SIPRI good practice guide aims to strengthen national efforts by PMP Code of Practice supporters by clarifying how export controls can be applied to CCICs and informing multilateral discussions on using export controls to tackle their proliferation and misuse.

INTRODUCTION

The Pall Mall Process (PMP) was launched by France and the United Kingdom in 2024 to tackle the challenges posed by the 'proliferation and irresponsible use' of commercial cyber intrusion capabilities (CCICs).[1] The process led to the adopting in April 2025 of the PMP Code of Practice for States. The PMP code of practice is a voluntary and non-binding agreement that seeks to build on aspects of international law, including human rights treaties and standards, to specify how states should act when developing, transferring, acquiring and using CCICs.[2] States endorsing the PMP code of practice commit to using export controls to help ensure accountability across the market for CCICs and 'to mitigate risks of potential irresponsible use' of CCICs.[3]

The PMP code of practice emphasizes that export controls are only one component of an effective policy response to the challenges posed by the proliferation and misuse of CCICs. Other relevant tools include sanctions measures, investment screening tools and robust standards for the development, acquisition and use of CCICs. However, export controls are an important aspect of an effective response. They can give states the ability to regulate transfers of certain types of CCICs, improve oversight of the trade in CCICs, and prevent transfers of CCICs that threaten human rights and national security.

States supporting the PMP code of practice have committed to 'Exploring opportunities for needs-based capacity building support to address the technical challenges presented by the implementation and enforcement of controls.'[4] This SIPRI good practice guide seeks to strengthen these

[1] British Foreign, Commonwealth and Development Office (FCDO), 'The Pall Mall Process declaration: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities' (PMP declaration), 6 Feb. 2024.

[2] British FCDO, 'The Pall Mall Process Code of Practice for States' (PMP code of practice), 25 Apr. 2025.

[3] The states that have endorsed the PMP code of practice are Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Ghana, Greece, Hungary, Ireland, Italy, Japan, Kosovo, Latvia, Luxembourg, Moldova, the Netherlands, Poland, Republic of Korea, Romania, Slovakia, Slovenia, Sweden, Switzerland, the United Kingdom and the United States.

[4] British FCDO, PMP code of practice (note 2), para. 8.b.v.

* This publication was produced by SIPRI with financial support from the UK Foreign, Commonwealth and Development Office.

efforts by helping PMP code of practice supporters—whose resources and needs may differ—to operationalize the document's export control–related commitments. It draws from the experiences of states and the expertise of government officials, company representatives, academics and non-governmental organization (NGO) experts, as well as the content of available guidance materials and policy documents.

The guide begins with an outline of the key elements of multilateral export control frameworks that states can use when regulating transfers of CCICs (section II). It then describes specific aspects of applying export controls to transfers of CCICs: establishing controls on transfers of CCICs (section III); informing exporters of CCICs of their licensing obligations (section IV); applying end-use/end-user controls to transfers of CCICs (section V); and publishing information on the application of controls on transfers of CCICs (section VI). Each of sections III–VI highlights the commitments that PMP code of practice supporters have made, the types of challenges that this aspect of applying export controls to transfers of CCICs presents, and steps states could take at the national and multilateral levels.

EXISTING MULTILATERAL EXPORT CONTROL FRAMEWORKS

There are two multilateral instruments which are particularly relevant for establishing standards that can form the basis for national export controls on CCICs.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement) was established in 1996 to promote 'transparency and greater responsibility' regarding transfers of military and dual-use items.[5] It has 42 participating states.[6] The Wassenaar Arrangement has developed standards for the coverage of export controls and export licensing criteria, which states can use to control transfers of CCICs.

The European Union (EU) dual-use regulation establishes common standards among EU member states for controls on the export, re-export, brokering, technical assistance, transit and transfer of dual-use goods, software and technology.[7] The regulation adopts and expands on the Wassenaar Arrangement's standards, making them directly applicable law in all EU member states.

The Wassenaar Arrangement and the EU dual-use regulation have also established mechanisms for exchanging information on export controls.

[5] Wassenaar Arrangement, 'About us', [n.d.] <http://www.wassenaar.org/about-us/>.

[6] These states are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, the UK and the USA. Wassenaar Arrangement, 'About us' (note 5).

[7] 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 (recast) (EU dual-use regulation), *Official Journal of the European Union*, L206, 11 June 2021.

Standards for the coverage of export controls

The Wassenaar Arrangement maintains control lists for military and dual-use items. The Wassenaar dual-use list includes physical goods as well as certain 'intangible' items that can be transferred via 'intangible' means. These include different types of types of software, technical data and technical assistance which can be transferred orally, via email or via cloud servers.

Annex I of the EU dual-use regulation (the 'EU dual-use list') outlines the items that are subject to control under the regulation. The EU dual-use list integrates the control lists adopted by the four multilateral export control regimes, including the Wassenaar Arrangement.

At least 22 states that are not Wassenaar participating states or EU member states apply the Wassenaar or EU dual-use lists in their export controls.[8]

States also use 'catch-all controls' to capture exports of items that are not covered by their control lists (so-called 'unlisted items') but which raise human rights or national security concerns. Catch-all controls take effect when a national authority informs an exporter that they require a licence or when an exporter asks their national authority if they require a licence. Article 5 of the EU dual-use regulation establishes a catch-all control for unlisted cyber-surveillance items. (The regulation 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'.) Article 5 applies to exports of unlisted cyber-surveillance items which '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'.[9]

Standards in export licensing criteria

The Wassenaar Arrangement recommends that states exporting conventional weapons consider whether there is 'a clearly identifiable risk that the weapons might be used to commit or facilitate the violation and suppression of human rights and fundamental freedoms or the laws of armed conflict'.[10] However, there is no equivalent recommendation for exports of dual-use items.

The EU dual-use regulation and the EU common position on arms exports require EU member states to apply the criteria of the EU common position when issuing export licences for dual-use items for transfers to 'the armed forces or internal security forces or similar entities in the [recipient] country'.[11] This process involves three key dimensions: assessing the recipient

[8] These include Israel (Wassenaar dual-use list) and Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Cyprus, Georgia, Jordan, Kazakhstan, Kosovo, Laos, Malaysia, Moldova, Montenegro, North Macedonia, Pakistan, Panama, Philippines, Serbia, Singapore, Thailand and the United Arab Emirates (EU dual-use list). See Privacy Shield Framework, 'Israel: US export controls', *Israel Country Commercial Guide*, [n.d.]; and Michel, Q. and Paile, S., 'Countries having adopted the EU dual-use list as national control list', Working document, University of Liege, May 2021.

[9] EU dual-use regulation (note 7), Article 2(20) .

[10] Wassenaar Arrangement, 'Elements for objective analysis and advice concerning potentially destabilising accumulations of conventional weapons', Explanatory note, 2011, para. 1(c).

[11] EU dual-use regulation (note 7), Article 15(1); and Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment (EU common position), *Official Journal of the European Union*, L335, 8 Dec. 2008, Article 6.

country's human rights record; exercising special caution and vigilance; and, if necessary, denying export licences. In respect of each dimension, the EU common position states that EU member states shall:

1. Assess (*a*) 'the recipient country's attitude towards relevant principles established by international human rights instruments', (*b*) 'the human rights situation in that country', and (*c*) 'the recipient country's attitude towards relevant principles established by instruments of international humanitarian law and respect for international humanitarian law'.[12]
2. Having undertaken the assessments, 'exercise special caution and vigilance in issuing licences . . . to countries where serious violations of human rights have been established by the competent bodies of the United Nations, by the European Union or by the Council of Europe'.[13]
3. Having undertaken the assessments, deny export licences if there is a 'clear risk' that the item 'might be used' to 'commit' or 'facilitate' (*a*) 'internal repression, serious acts of gender-based violence or serious acts of violence against women, children, or other serious violations of human rights', or (*b*) 'serious violations of international humanitarian law, including against protected groups under international humanitarian law, such as women and children'.[14]

Mechanisms and forums for exchanging information on export controls

Wassenaar participating states share information on denials of dual-use export licences for transfers to non-participants. They also present and discuss potential amendments to the Wassenaar Arrangement control lists via the Experts Group and aspects of export control enforcement via the Licensing and Enforcement Officers Meeting.

Under the EU dual-use regulation, EU member states share information on all approvals and denials of export licences for dual-use items. EU and EU member state officials discuss the implementation of the EU dual-use regulation in the Dual-use Working Party chaired by the European Council and the Dual-use Coordination Group chaired by the European Commission. EU and EU member state officials also meet in five expert groups with a focus on issues relevant to applying export controls to transfers of CCICs:

- the Surveillance Technology Expert Group, which focuses on 'the development of EU controls on exports of cyber-surveillance items';[15]

[12] EU common position (note 11), Article 2(2).
[13] EU common position (note 11), Article 2(2)(b).
[14] EU common position (note 11), Article 2(2)(a) and (c).
[15] European Commission, 'Report from the Commission to European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', COM(2025) 19 final, 30 Jan. 2025, para. 3.3(a).

- the Enforcement Coordination Mechanism, which focuses on 'the detection and prosecution of unauthorised exports of dual-use items';[16]
- the Technical Expert Group on Data Collection and Transparency, which focuses on methodologies 'to collect and report licensing data' and guidelines for transparency;[17]
- the Technical Expert Group on Capacity-Building (CB-TEG), which supports 'regular training and sharing of expertise within the EU dual-use community, including through developing common training programmes for Member States' officials';[18] and
- the Technical Expert Group on Intangible Technology Transfers, which supports the development of guidelines for issues related to controls on transfers of intangible technology.[19]

The standards outlined in the Wassenaar Arrangement and the EU dual-use regulation are applied through states' national laws and export control systems. This leads to differences in interpretations and applications of control list categories, catch-all controls and export licensing criteria; the level of evidence required for an export licence denial to be issued; and the ability and willingness of states to deny export licences. The standards are also intended to be a floor and not a ceiling. Wassenaar participating states and EU member states can adopt additional control list categories, catch-all controls and export licensing criteria. The EU dual-use regulation allows EU member states to adopt national controls on items that are not captured by the EU dual-use list 'for reasons of public security, including the prevention of acts of terrorism, or for human rights considerations'.[20]

ESTABLISHING CONTROLS ON TRANSFERS OF CCICS

PMP code of practice supporters have made three commitments relevant to establishing controls on transfer of CCICs:

- Establishing or applying national frameworks to the extent possible in relation to the . . . transfer . . . of CCICs.
- Applying controls, where applicable, on the export of CCICs . . .
- Exploring opportunities to update multilateral or domestic export control regimes to ensure appropriate coverage of CCICs.[21]

In practice, establishing controls on transfers of CCICs involves (*a*) defining what items are covered by CCICs, (*b*) adopting appropriate list-based controls, (*c*) adopting appropriate catch-all controls, and (*d*) framing and applying controls on intangible items.

[16] EU dual-use regulation (note 7), Article 25(2).
[17] European Commission, COM(2025) 19 final (note 15), para. 3.3(d).
[18] European Commission, COM(2025) 19 final (note 15), para. 3.3(e)-7.
[19] Government official, Communication with the authors, 6 Feb. 2026.
[20] EU dual-use regulation (note 7), Article 9.
[21] British FCDO, PMP code of practice (note 2), paras 8.a, 8.b and 8.b.iv.

Defining what items are covered by CCICs

The PMP code of practice does not include a definition of CCICs. Officials associated with the PMP have indicated that the focus of attention is on three categories of CCICs: spyware; hackers-for-hire services and hacking as a service; and software vulnerabilities and exploits that underpin cyber intrusion activity.[22] Box 1 gives definitions of these three categories of CCICs.

A set of 'working definitions' circulated in advance of a February 2024 meeting of the PMP noted that 'Commercially available cyber intrusion capabilities describe tools and services made available by cyber intrusion companies and similar high-end capabilities developed by other companies.'[23] It also highlighted the importance of 'capability providers' that operate on an 'access-as-a-service' model 'whereby one entity provides the access vector by which end-users are able to gain unauthorised access to computer systems'.[24] These 'working definitions' indicate that states should take a wider view of what counts as CCICs and include other tools and technologies which support the deployment of spyware or have similar capabilities to spyware.[25] For example, there is evidence that states have used mobile phone interception equipment and digital forensics systems to facilitate the deployment of spyware.[26] There is also evidence that monitoring centres can provide states with a similar level of access to communications data as spyware enables.[27] Box 2 gives definitions of these three related surveillance tools.

Adopting appropriate list-based controls

Systems that employ a certain standard of encryption, or that enable the decryption of encrypted data, are included in the Wassenaar and EU dual-use lists. Certain types of CCICs and related tools may be captured by these controls because of the level of encryption that they use or their ability to decrypt encrypted data.[28] Since 2012, list-based controls have been added to the Wassenaar and EU dual-use lists that capture transfers of certain types of spyware, software vulnerabilities and exploits, mobile phone interception equipment, digital forensics systems and monitoring centres. The scope of these controls is discussed in boxes 1 and 2.

The controls added to the Wassenaar and EU dual-use lists only apply if the national authorities assess that the exported item meets the technical standards described in the relevant control list category. This means that CCICs that perform the functions described in boxes 1 and 2 might not be

[22] Statements made by British and French officials at the Second Pall Mall Process Conference, Paris, 3–4 Apr. 2025.

[23] British FCDO, (PMP declaration) (note 1), Annex A para. 1.

[24] 'British FCDO, (PMP declaration) (note 1).

[25] NGO expert, Interview with the authors, 1 Dec. 2025.

[26] Amnesty International, Security Lab, 'Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products', 6 Oct. 2023; and Amnesty International, 'Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists', 16 Dec. 2024,.

[27] Amnesty International, 'Pakistan: Mass surveillance and censorship machine is fueled by Chinese, European, Emirati and North American companies', 9 Sep. 2025.

[28] Council of the European Union, 'Guidelines on the export of cyber-surveillance items under Article 5 of the Regulation (EU)2021/821 of the European Parliament and of the Council', 14507/24, 15 Oct. 2024, p. 19.

controlled if they do not meet these technical standards (although such transfers might be captured by the encryption and decryption controls).[29] There have been reports of companies transferring digital forensics tools that do not meet the technical standards specified in the Wassenaar and EU dual-lists and that do not require an export licence.[30]

Controlling transfers of CCICs via catch-all controls

Catch-all controls can be used to capture transfers of CCICs that do not meet the technical standards outlined in the Wassenaar and EU dual-use list. The EU dual-use regulation's Article 5 catch-all control could be used to capture such transfers. However, since its introduction there have been no reports of any EU member state applying the Article 5 catch-all control by notifying an exporter of the need to apply for a licence or of a company notifying a member state of the potential need to do so.[31] The limited use of the Article 5 catch-all control might reflect the way it is framed. The control only applies if (*a*) the item being transferred fits the EU dual-use regulation's definition of cyber-surveillance items; and (*b*) the item 'may be intended, in [its] 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'.[32]

In 2022 the UK amended its existing military end-use catch-all controls. The amended controls allow the national authority to apply controls to non-listed items which 'are or may be intended for use by a "relevant entity"', defined to include 'any military forces, para-military forces, police forces, security services or government intelligence organisations of an embargoed destination' and 'any person or entity involved in the procurement, research, development, production or use of items on behalf of the entities above'.[33] The UK also added China to its list of 'embargoed destinations'.[34] According to a British official, these amended catch-all controls have been used to capture exports of different types of surveillance technologies and could be a means of preventing exports of CCICs that pose risks of diversion or misuse.[35]

Framing and applying controls on 'intangible transfers'

Many exports of CCICs involve the cross-border movement of 'intangible' items, particularly software, that can be transferred, stored and shared electronically. Some types of CCICs can be transferred or made available using cloud servers. There are also cases of companies making CCICs available to vendors in a software-as-a-Service (SaaS) model, where vendors

[29] Council of the European Union, 'Guidelines on the export of cyber-surveillance items under Article 5 of the Regulation (EU)2021/821 of the European Parliament and of the Council', 14507/24, 15 Oct. 2024, p. 19.

[30] Campbell, Z. and Chandler, C. L., 'Tools for repression in Myanmar expose gap between EU tech investment and regulation', *The Intercept*, 14 June 2021.

[31] Bromley, M. and Maletta, G., 'Export controls and spyware: Enhancing oversight, transparency and restraint', SIPRI Policy Paper, Sep. 2025, p. 16.

[32] EU dual-use regulation (note 7), Article 5.

[33] British Export Control Joint Unit, 'End-use controls applying to military related items', Guidance, 14 Apr. 2023.

[34] British Export Control Joint Unit (note 33).

[35] British government official, Interview with the authors, 3 Dec. 2025.

Box 1. Commercial cyber intrusion capabilities (CCICs) and their inclusion in the Wassenaar and European Union (EU) dual-use lists

For the control list categories mentioned, see the Wassenaar Arrangement's 2025 dual-use goods and technologies list and munitions list.[a]

Spyware

Description. Spyware refers to 'commercially-available software and tools that provides the user the capability to gain remote access to a computer system, without the consent of the user, administrator, or owner of the computer system, in order to access, collect, exploit, extract, intercept, retrieve, alter or delete or transmit content, including information stored on or transmitted through a device connected to the Internet. This may include the capability to record video, audio or calls, or to track the location of the computer.'[b]

Inclusion in the Wassenaar and EU dual-use lists. Exports of certain types of spyware are captured by controls on 'systems, equipment, and components', 'software' and 'technology' that is 'specially designed' for the 'generation, command and control, or delivery' of 'intrusion software' (4.A.5, 4.D.1, and 4.E.5) which were added to the Wassenaar dual-use list in 2013 and the EU dual-use list in 2014. The Wassenaar and EU dual-use lists define 'intrusion software' as software that is 'specially designed or modified to avoid detection by "monitoring tools", or to defeat "protective countermeasures", of a computer or network-capable device' to remotely extract or modify data and, in some cases, take control of the device.[c]

Hackers-for-hire services and hacking as a service

Description. Hackers-for-hire services and hacking as a service refer to the provision of 'computer system penetration to meet customer requirements', where the service providers are companies, individuals or groups of individuals.[b]

Inclusion in the Wassenaar and EU dual-use lists. Export controls only apply if there are cross-border movements of controlled items, which would not necessarily be the case for hackers-for-hire services and hacking as a service. The controls on 'technical assistance' in the Wassenaar and EU dual-use lists could create a means for regulating certain aspects of hackers-for-hire services and hacking as a service. These controls capture the provision of 'instruction, skills, training, working knowledge, consulting services' that is ' "required" for the "development", "production" or "use" of' items on the Wassenaar and EU dual-use lists. Routine technical support is not covered by the Wassenaar and EU controls on technical assistance.

Germany has included controls on 'technical support' for previously exported surveillance tools in its national dual-use export controls.[d] These controls could make the provision of a wider set of activities related to hackers-for-hire services and hacking as a service subject to export controls. However, a national official noted that export controls, which are primarily focused on transfers of controlled items, are limited in their ability to capture services, and that it might be better to regulate hackers-for-hire services and hacking as a service through other instruments.[e] Switzerland and several other states have licensing systems to regulate the actions of private security firms.[f] These systems could provide an alternative means for controlling hackers-for-hire services and hacking as a service.

Software vulnerabilities and exploits

Description. A software vulnerability 'is a weakness, or flaw, in a system or process' and an exploit is code that has been developed 'to exploit a vulnerability to gain access to a system'.[b]

Inclusion in the Wassenaar and EU dual-use lists. Some governments have indicated that transfers of software vulnerabilities and exploits are captured by controls on 'systems, equipment, and components', 'software' and 'technology' that are 'specially designed' for the 'generation, command and control, or delivery' of 'intrusion software' (4.A.5, 4.D.1, and 4.E.1.c).[g] A government official indicated that these controls capture transfers of software vulnerabilities and exploits unless they are connected to processes of 'vulnerability disclosure', through which software vulnerabilities are identified and reported.[h] A representative of a company that develops software vulnerabilities and exploits for use by governments and private companies in the development and deployment of spyware indicated that these controls cover exports of these tools.[i]

[a] Wassenaar Arrangement, *Public Documents Volume II: List of Dual-Use Goods and Technologies and Munitions List*, 5 Dec. 2025.

[b] British Foreign, Commonwealth and Development Office, 'The Pall Mall Process declaration: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities', 6 Feb. 2024.

[c] Wassenaar Arrangement (note a), p. 224.

[d] German Federal Ministry for Economic Affairs and Energy (BMWI), 'BMWI: Stärkere Kontrollen beim Export von Überwachungstechnologie' [BMWI: Stronger controls on the export of surveillance technology], 15 July 2015.

[e] Government official, Interview with the authors, 4 Dec. 2025.

[f] See Swiss Federal Department of Foreign Affairs, 'Federal Act on Private Security Services Provided Abroad (PSSA)', [n.d.].

[g] See British Export Control Organisation, 'Intrusion software tools and export control', Notice to Exporters, 10 Aug. 2015.

[h] Government official, Interview with the authors, 3 Dec. 2025.

[i] Company representative, Interview with the authors, 27 Nov. 2025.

Box 2. Other surveillance tools related to commercial cyber intrusion capabilities (CCICs) and their inclusion in the Wassenaar and European Union (EU) dual-use lists

For the control list categories mentioned, see the Wassenaar Arrangement's 2025 dual-use goods and technologies list and munitions list.[a]

Mobile phone interception equipment

Description. Mobile phone interception equipment is used to remotely track, identify, intercept and record mobile phones.[b] The most widely cited example is international mobile subscriber identity (IMSI) catchers, which mimic the functionality of a mobile phone tower in order to extract data from mobile phones.[c]

Inclusion in the Wassenaar and EU dual-use lists. Exports of certain types of mobile phone interception equipment are captured by controls on 'mobile telecommunications interception or jamming equipment' (5.A.1.f.), which were added to the Wassenaar dual-use list in 2012 and the EU dual-use list in 2013. The controls capture IMSI catchers and equipment that create fake Wi-Fi hotspots for surveillance purposes, as well as 'certain types of items specially designed to enable "deep packet inspection" into telecommunications systems'.[d]

Digital forensics systems

Description. Digital forensics systems are used by law enforcement agencies (LEAs) or intelligence agencies to retrieve and analyse data stored on networks, computers and mobile devices.[e]

Inclusion in the Wassenaar and EU dual-use lists. Exports of certain types of digital forensics systems are captured by controls on systems that can ' "Extract raw data" from a computing or communications device' and 'Circumvent [the] "authentication" or authorisation controls of the device' (5.A.4.b), which were added to the Wassenaar dual-use list in 2019 and the EU dual-use list in 2020.

Monitoring centres

Description. Monitoring centres are used by LEAs and intelligence agencies to collect, store and analyse different forms of communications data from various surveillance sources.[f]

Inclusion in the Wassenaar and EU dual-use lists. Exports of certain types of monitoring centres are captured by controls on software 'for monitoring or analysis for law enforcement purposes' (5.D.1.e), which were added to the Wassenaar dual-use list in 2019 and the EU dual-use list in 2020. The controls apply to software used by LEAs and intelligence agencies to analyse communications data or metadata provided by a communications service provider.

[a] Wassenaar Arrangement, *Public Documents Volume II: List of Dual-Use Goods and Technologies and Munitions List*, 5 Dec. 2025.
[b] Access Now, 'New paper recommends how to keep surveillance tech from human rights abusers', 13 Mar. 2015.
[c] Privacy International, 'IMSI catchers', Explainer, 6 Aug. 2018.
[d] Council of the European Union, 'Guidelines on the export of cyber-surveillance items under Article 5 of the Regulation (EU) 2021/821 of the European Parliament and of the Council', 14507/24, 15 Oct. 2024, p. 17.
[e] See Interpol, 'Digital forensics', [n.d].
[f] Privacy International, 'Monitoring centres: Force multipliers from the surveillance industry', 29 Apr. 2014.

make software applications available to users via cloud servers without the user having to download them.[36]

States differ in their understandings of how export controls apply when technology or software subject to export controls are transferred using cloud servers or when an end-user is given access to controlled software in an SaaS model.[37] These differences revolve around who is viewed as the exporter; which part of the transaction triggers an export licensing requirement; and, in the case of SaaS, whether accessing but not downloading software is viewed as an export.[38] The decisions states make about how export controls

[36] See Brockmann, K. and Héau, L., 'Spyware as a service: Challenges in applying export controls to cloud-based cyber-surveillance software', SIPRI Topical Backgrounder, 17 Feb. 2025.
[37] Brockmann and Héau (note 36).
[38] Brockmann and Héau (note 36).

are framed and applied in these areas will affect their ability to require companies to apply for export licences if they are transferring CCICs using cloud servers or providing an end-user with access to CCICs in an SaaS model.

Good practices for establishing controls on transfers of CCICs

PMP code of practice supporters could adopt the following good practices:

- Adopt and apply control list categories from the Wassenaar and EU dual-use lists and catch-all controls to regulate transfers of CCICs.
- Use EU and PMP forums to share information on the interpretation and application of the Wassenaar and EU dual-use lists and catch-all controls to transfers of different types of CCICs.
- Use EU and PMP forums to exchange information with other states and NGOs to help identify transfers of CCICs that are not captured by the Wassenaar and EU dual-use lists.
- Use EU forums to amend the Article 5 catch-all control to capture CCICs that fall outside the scope of the EU dual-use list.
- Use PMP forums to promote the wider use of catch-all controls to capture CCICs that fall outside the scope of the Wassenaar and EU dual-use lists.
- Use Wassenaar, EU and PMP forums to share information on the use of export controls and other policy instruments to regulate hackers-for-hire services and hacking as a service.
- Review national policies regarding the application of export controls to cloud servers and SaaS models and assess how this affects the ability to regulate transfers of CCICs.
- Use Wassenaar, EU and PMP forums to exchange information on cases where CCICs are being shared via cloud servers or where an end-user is being given access to CCICs in an SaaS model.
- Use Wassenaar and EU forums to adopt new list-based and catch-all controls to capture transfers of CCICs that fall outside the scope of the Wassenaar and EU dual-use lists.

INFORMING CCIC EXPORTERS OF THEIR LICENSING OBLIGATIONS

PMP code of practice supporters have made the following commitment relevant to informing exporters of CCICs of their licensing obligations:

- Reviewing, and where necessary preparing, published guidance to ensure it clarifies where and how States existing domestic export control regulations place obligations on exporters, including the consequences of non-compliance with these obligation.[39]

[39] British FCDO, PMP code of practice (note 2), para 8.b.iii.

Outreach and awareness-raising activities are an essential component of an effective export control system. This is particularly important for providers of CCICs who might have limited awareness of export control obligations and rarely engage with export control authorities. There are also many open questions about the scope of export control measures that might apply to the tools they provide. Outreach and awareness-raising activities should focus on (*a*) identifying possible exporters of CCICs, and (*b*) making possible exporters of CCICs and other relevant stakeholders aware of their export control obligations.

Identifying possible exporters of CCICs

The range of companies that develop, test, produce and export CCICs is not a homogeneous group but rather an assortment of different types of companies, from small start-ups to major software providers. Some companies view themselves as part of the cyber-security sector, while others explicitly do not identify with this sector. As a result, there are few, if any, industry or professional associations that bring together the most relevant providers of CCICs and associated products, services, software and technology in each state or region. Many CCIC providers appear to avoid the possible attention that might result from participation in larger public export control conferences and other events.

Possible methods for identifying current and potential exporters of CCICs include: researching CCIC markets; mapping company registries and membership lists of relevant industry and professional associations; and investigations conducted by enforcement and intelligence services. States can also use previous studies on the scope and content of the 'surveillance industry', the 'spyware market' or the information and communications technology (ICT) sector more broadly.[40] Commercial trade databases can also be used to identify cases in which companies involved in the production of CCICs are exporting items to different states.[41] These types of transactions can provide an indication that exports of controlled items may have taken place.

Another key method is to work with other government agencies that have connections to these companies, as either a regulator or a customer. One government official noted that they had benefited from close cooperation with their national cybersecurity agency when mapping companies that were possible exporters of CCICs.[42] In a different state, officials contacted the agencies responsible for the procurement of surveillance tools used by the national military and law enforcement agencies (LEAs) to map possible exporters of items captured by the EU dual-use regulation.[43]

[40] These include Privacy International, *The Global Surveillance Industry* (Privacy International: Oxford, July 2016); Feldstein, S. and Kot, B., 'Mapping the shadowy world of spyware and digital forensics sales', Dataset Carnegie Endowment for International Peace, 27 Feb. 2023; Roberts, J. et al., *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights* (Atlantic Council: Washington, DC, 4 Sep. 2024); 'Technology company dashboards', Business and Human Rights Centre, Mar. 2025; and 'Surveillance Watch', Database, [n.d.].

[41] See Amnesty International, 'Pakistan: Mass surveillance and censorship machine is fueled by Chinese, European, Emirati and North American companies' (note 27).

[42] Government official, Interview with the authors, 3 Dec. 2025.

[43] Government official, Interview with the authors, 4 Dec. 2025.

Making possible exporters of CCICs and other relevant stakeholders aware of their export control obligations

Dedicated outreach events targeting providers of CCICs are a proactive way of engaging these actors or sub-groups within them, such as start-ups. Targeted outreach events can be conferences, workshops, seminars or webinars. These events can bring together companies that require information about export controls and companies that can share experiences to the benefit of others. Ad hoc events, such as company visits, can also be organized to address more specific questions and issues, or to put a company otherwise avoiding engagement through other outreach formats on the spot. Another way of engaging key stakeholders, including CCIC providers and possible resellers, is for export licensing authorities to participate in industry events by, for example, providing a presentation on export controls, operating a booth, or engaging in conversation and discussion with participants from the sector.

Outreach can also involve producing targeted guidance materials that clarify aspects of export controls. Companies and researchers working in the ICT sector have pointed to a lack of clarity about which transfers are covered by the control list items outlined in boxes 1 and 2. Specific concerns have been raised about the controls on 'systems, equipment, and components', 'software' and 'technology' that is 'specially designed' for the 'generation, command and control, or delivery' of 'intrusion software' (4.A.5, 4.D.1, and 4.E.1.c) adopted by the Wassenaar Arrangement and the EU dual-use regulation. One concern is that these controls capture processes that are essential to ICT security, including tools and techniques associated with penetration testing, in which attacks on ICT systems are simulated to test their weaknesses, and processes of vulnerability disclosure.[44] Providing more granular guidance can help reduce adverse consequences for cybersecurity work, without reducing the scope of applicable controls.

In 2015 the British Export Control Organisation published guidance to clarify the scope of controls on 'intrusion software tools'.[45] This remains the only national guidance document that is specifically focused on the scope of 4.A.5, 4.D.1, and 4.E.1.c. In 2017 explanatory notes were added to the Wassenaar dual-use list, specifying that the controls in 4.E.1.a and 4.E.1.c do not apply to 'vulnerability disclosure' and 'cyber incident response' processes.[46] Since 2013 Germany, the EU and the Netherlands have published guidelines aimed at supporting exporters' implementation of the EU dual-use regulation's Article 5 catch-all control.[47] The guidelines contain information on the scope of 4.A.5, 4.D.1 and 4.E.1.c and the other controls listed in boxes 1 and 2.

Despite these developments, companies and researchers continue to maintain that there are uncertainties about the coverage of 4.A.5, 4.D.1 and 4.E.1.c. A specific concern is the lack of clarity about how the controls apply

[44] Bratus, S., Locasto, M. and Shubina, A., 'Why Wassenaar Arrangement's definitions of "intrusion software" and "controlled items" put security research and defense at risk', *;login:*, vol. 39, no. 4 (2014).

[45] British Export Control Organisation, 'Intrusion software tools and export control', Notice to Exporters, 10 Aug. 2015.

[46] Wassenaar Arrangement, *Public Documents Volume II: List of Dual-Use Goods and Technologies and Munitions List*, 5 Dec. 2025, p. 81.

[47] German Federal Office for Economic Affairs and Export Control (BAFA), 'Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)', Oct. 2021; Council of the European Union (note 28); and Dutch Ministry of Foreign Affairs, 'Export controls for cyber-surveillance items: A focus on protecting human rights', Leaflet, 5 Jan. 2025.

to more dynamic aspects of cyber-security work, such as the identification of software vulnerabilities and the development of exploits for the purposes of testing a client's cybersecurity standards, without necessarily leading to a process of 'vulnerability disclosure'.[48] A representative of a company that exports software vulnerabilities and exploits indicated that they had benefited from having direct contact with officials at their national licensing authority who were able to clarify the scope of these controls.[49]

Companies and researchers working in the ICT sector have also highlighted the lack of clarity and alignment in how states apply export controls when software or technology is shared via cloud servers or when software is made available in SaaS models. Some national governments have published guidance to clarify these aspects of export controls.[50] However, many states have not published any public guidance on these issues. The EU is currently working on common guidelines on the implementation of controls on intangible transfers of technology among member states. These guidelines are expected to address the question of how export controls apply when software or technology is shared via cloud servers.[51]

Good practices for informing exporters of CCICs of their licensing obligations

PMP code of practice supporters could adopt the following as good practices:

- Map companies that may be developing, testing, producing and exporting CCICs through researching CCIC markets and engagement with industry, NGO experts tracking human rights violations, and relevant government agencies.
- Conduct targeted outreach to companies that are developing, testing, producing and exporting CCICs through dedicated events, participation at industry events and targeted company visits.
- Publish information on concluded enforcement actions to demonstrate the consequences of violations and the penalties applied.
- Publish national guidelines detailing which technologies and transfers are covered by control list categories, particularly 4.A.5, 4.D.1 and 4.E.1.c.
- Use Wassenaar Arrangement, EU and PMP forums to develop joint guidelines detailing which technologies and transfers are covered by control list categories, particularly 4.A.5, 4.D.1 and 4.E.1.c. Where appropriate, include opportunities for stakeholder consultation in the process of developing such guidelines.

[48] Company representative, Interview with the authors, 13 Jan. 2026.
[49] Company representative, Interview with the authors, 27 Nov. 2025.
[50] See Dutch Ministry of Foreign Affairs, 'Export naar de Cloud' [Export to the cloud], Factsheet, 23 Oct. 2018; and BAFA, 'Immaterieller Technologietransfer (ITT)' [Intangible technology transfer (ITT)], May 2024.
[51] See European Commission, COM(2025) 19 final (note 15), para. 3.2.

- Publish national guidelines detailing how export controls apply to cases where software or technology is transferred via cloud servers and when an end-user is given access to controlled software in an SaaS model.
- Use EU forums to develop joint guidelines detailing how export controls apply to cases where software or technology is transferred via cloud servers and when an end-user is given access to controlled software in an SaaS model.

APPLYING END-USE/END-USER CONTROLS TO TRANSFERS OF CCICS

PMP code of practice supporters have made the following commitments relevant to applying end-use/end-user controls to transfers of CCICs:

- Ensuring export control licensing decisions concerning CCICs take into account the risk, among others, of their use in connection with internal repression, as appropriate, and/or the commission of serious violations or abuses of human rights.
- Ensuring licensing decisions limit the export of CCICs to a specific end-user and for a defined lawful and legitimate purpose, and where consideration of these elements does not raise concerns regarding lawful and responsible use or the risk of diversion.
- Exploring opportunities to encourage CCIC vendors to conduct human rights due diligence, in order to identify, prevent and mitigate their adverse human rights impacts.[52]

End-use/end-user controls are efforts by exporting states to prevent cases of diversion or misuse of controlled items. They can lead to an export licence denial or can be used to impose restrictions on how, where and by whom exported items are used after delivery.[53] Effective end-use/end-use controls require the active cooperation of exporters, who have first-hand information on technical developments that might generate new risks of diversion and on inquiries and procurement attempts that raise possible red flags.[54] For these reasons, most states share the view that exporters should act as the first line of defence in preventing diversion and misuse of controlled items. States thus seek to require or incentivize exporters to adopt comprehensive internal compliance programmes (ICPs) and due-diligence processes.

Applying effective end-use/end-user controls to exports of CCICs requires states to have (*a*) clear export licensing criteria and decision-making powers, (*b*) effective and adequately resourced systems for collecting and assessing information about transfers, and (*c*) appropriate and effective post-shipment measures.

[52] British FCDO, PMP code of practice (note 2), paras 8.b.1, 8.b.ii and 8.c.iv.

[53] Wassenaar Arrangement, 'Introduction to end user / end use controls for exports of military-list equipment', 3 July 2014.

[54] Viski, A. and Jones, S., *Outreach 2.0: Emerging Technologies and Effective Outreach Practices* (Strategic Trade Research Institute: Washington, DC, Feb. 2021), p. 10.

Clear export licensing criteria and decision-making powers

The human rights violations that have been associated with the use of CCICs range from infringements of the right to life, privacy, freedom of expression and freedom of association, to breaches of 'non-derogable' and 'inviolable' rights, such as freedom from torture and inhuman or degrading treatment.[55] International organizations and NGOs have raised concerns about the potential of CCICs to facilitate attacks on civilians during armed conflicts.[56] There is also evidence that women are particularly prone to risks of harm associated with the deployment of targeted digital surveillance tools without adequate legal and ethical safeguards.[57] CCICs also raise a range of national security concerns, including their potential uses in enabling the theft of government and commercial secrets, attacks on critical infrastructure and the support of military operations.[58]

The human rights criteria outlined in the EU dual-use regulation and EU common position provide language that reflects these human rights risks and concerns. However, these instruments are predominantly focused on risks related to the export and use of military equipment and weapons of mass destruction, rather than on the oversight measures recipient states should have in place to ensure that CCICs are only used for a 'lawful and legitimate purpose'.[59] Efforts to develop clearer standards in this area, such as the PMP code of practice standards for the responsible acquisition and use of CCICs, could form the basis for states' risk assessment criteria for export licences.

The EU dual-use regulation specifies that the human rights risks assessments should only be applied to exports to 'armed forces or internal security forces or similar entities'.[60] Limiting the risk assessment process in this way means that exports to private companies that are developing CCICs, or deploying CCICs on behalf of a state, might not be subject to scrutiny. States have adopted national measures to ensure that risk assessment criteria relating to human rights apply to all exports of dual-use items. In 2015 the Swiss government introduced a new ordinance to its export controls which specified that permits for the export of 'goods intended for the surveillance of the Internet and mobile communications' will be refused 'if there is reason to believe that the goods will be used by the final recipient for the purposes of repression'.[61] In 2020 the US Department of Commerce's Bureau of

[55] United Nations, Office of the High Commissioner for Human Rights, 'Spyware and surveillance: Threats to privacy and human rights growing, UN report warns', Press release, 16 Sep. 2022.

[56] Rizk, J. and Cordey, S., 'What we don't understand about digital risks in armed conflict and what to do about it', *Humanitarian Law & Policy*, 27 July 2023.

[57] See UN Women and UN University Institute in Macau, *Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia* (UN Women Regional Office for Asia and the Pacific, 2024).

[58] See Clapper, J. R., US Director of National Intelligence, 'Worldwide threat assessment of the US intelligence community', Statement for the Record to the US Senate Select Committee on Intelligence, 23 Mar. 2013, pp. 1–3; Stein, J., 'New eavesdropping equipment sucks all data off your phone', *Newsweek*, 22 June 2014; Braccini, C. et al., *Battlefield Digital Forensics: Digital Intelligence and Evidence Collection in Special Operations* (NATO Cooperative Cyber Defence Centre of Excellence: Tallinn, 2016); and US Department of State, *United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-respecting Digital Future*, July 2024.

[59] British FCDO, PMP code of practice (note 2), para. 8.b.ii.

[60] EU common position (note 11), Article 6.

[61] Swiss Government, 'Ordonnance du 25 novembre 2020 sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles (OSIC)' [Ordinance on the export

Industry and Security issued a rule allowing it to review licence applications for any items against human rights concerns.[62] States can and do encourage companies that export items subject to export controls to conduct their own due diligence and to apply the standards outlined in the UN Guiding Principles on Business and Human Rights.[63]

In many states, the decision to deny an export licence can be challenged in court and the government might need to demonstrate that it is in line with the criteria outlined in the national legislation.[64] This may involve having to demonstrate that there was a risk that the exported item would have been used in connection with a serious violation of human rights or international humanitarian law. This can be difficult in the case of CCICs, since the connection between the item and a human rights violation might not be as direct as for other items covered by export controls, such as military equipment. The human rights criteria outlined in the EU common position specify that export licences should be denied if there is a 'clear risk' that the items 'might be used' to 'facilitate' human rights violations.[65] This language increases the scope to deny export licences since the nature of the connection between the item and the human rights violation is defined more broadly.

Systems for collecting and assessing information about the transfer

The Wassenaar Arrangement specifies the information that states should require as part of an export licence application. This includes a description of the item, such as its type, quantity, value, and weight; its specifications and performance characteristics; the applicant and the purchaser; and the end-user (if different from the purchaser) and the end-use.[66] States can require exporters to provide additional information that can help them to better understand the transfer and the risks that specific items might pose. For exports of CCICs, this information may include details of the contract with the end-user and any built-in safeguards that prevent the product from being diverted or misused.

Effective systems for assessing the risks associated with exports of controlled items require inter-ministerial processes in which different branches of government with relevant expertise can view applications and

and brokering of goods intended for the surveillance of the internet and mobile communications], 22 Nov. 2020.

[62] US Department of Commerce, Bureau of Industry and Security, 'Amendment to licensing policy for items controlled for crime control reasons', Final Rule, 6 Oct. 2020.

[63] See Dutch Ministry of Foreign Affairs, 'Internal compliance programme: Guidelines for compiling an internal compliance programme for strategic goods, torture goods, technology and sanctions', Dec. 2019; and United Nations, Office of the High Commissioner on Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework* (UN: New York, 2011).

[64] Swiss Federal Administrative Court 'Ablehnungsverfügung für die Ausfuhr von Softwarelösungen in die Türkei' [Rejection of the export of software solutions to Turkey], Judgement, 17 Apr. 2018; Swiss Federal Administrative Court, 'Ablehnungsverfügung für die Ausfuhr von Gütern der Telekommunikation nach China' [Rejection order for the export of telecommunications goods to China], Judgement, 19 Apr. 2018; and Frankfurt Administrative Court, 'Urteil vom 10.02.2022—5 K 533/18.F' [Judgement of 10.02.2022—5 K 533/18.F], 10 Feb. 2022.

[65] EU common position (note 11), Article 2(2)(a).

[66] Wassenaar Arrangement, 'Extreme vigilance: sub-set of Tier 2 (VSL) items "best practices" ', Wassenaar Arrangement Secretariat, *Public Documents, Volume III: Compendium of Best Practice Documents* (Wassenaar Arrangement, Dec. 2023), p. 53.

raise concerns about the risk of diversion or misuse. Most states also have a mechanism for elevating sensitive cases to a senior political level for a final decision. National officials noted that in the process of assessing licence applications for exports of CCICs, it is particularly useful to involve the ministry of foreign affairs, intelligence agencies and national embassies in the countries where end-users are located.[67]

National officials have also highlighted the importance of open-source information in assessing potential risks of diversion or mis-use.[68] A significant volume of published research highlights cases in which states have used CCICs in ways that contravene internationally agreed human rights standards.[69] Efforts have also been made to map the extent to which states have adopted appropriate systems of oversight to regulate the use of surveillance tools. For example, the European Commission for Democracy through Law has mapped states' legal frameworks for governing 'the use of spyware as a tool of targeted surveillance'.[70]

Determining whether a particular export of CCICs is captured by national list-based and catch-all controls, and assessing risks of diversion or misuse can be challenging for export control authorities. This is particularly true for smaller states that may not have access to relevant technical expertise or an embassy where the end-user is located. One official noted that their export control authority has recognized these challenges and is seeking to recruit an expert with the relevant technical expertise.[71] EU member states can share details about complex export control cases—including ones involving transfers of CCICs—with a pool of national experts that has been established to address such queries.[72] The EU dual-use regulation has committed the EU to developing export control–related training programmes for officials in EU member states, which are being advanced through the work of the CB-TEG.

An essential aspect of effective mechanisms for assessing export licence applications are systems for sharing quantitative and qualitative information about how states are applying controls at the national level. These exchanges range from sharing information about approvals and denials of export licences, to in-depth presentations of processes such as assessing a licence application or detecting and investigating an attempt to bypass national controls. Such exchanges can help states to develop an agreed understanding of which CCICs are captured by export controls and which transfers should be approved and which denied. They can also assist with detecting cases where exporters are seeking to bypass one state's export controls by channelling a transfer of CCICs through another state's export control system.

[67] See Perez, S. L. et al., *From Export Control to Unknown Exports: How the EU's Dual-use Regime Falls Short on Tackling Spyware* (Center for Democracy & Technology Europe: Brussels, Dec. 2025), p. 38.

[68] See Perez et al. (note 67), p. 34.

[69] Recent examples include Amnesty International, 'Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists' (note 26); and Amnesty International, 'Pakistan: Mass surveillance and censorship machine is fueled by Chinese, European, Emirati and North American companies' (note 27).

[70] Venice Commission of the Council of Europe, 'Report on a rule of law and human rights compliant regulation of spyware', [n.d.].

[71] Government official, Interview with the authors, 28 Nov. 2025.

[72] Government official, Interview with the authors, 12 Jan. 2025.

Appropriate and effective post-shipment measures

End-use/end-user controls are implemented through a range of measures. These include inserting language into the end-user certificates (EUCs) or end-user statements (EUSs) attached to a transfer that commits the end-user to abide by certain restrictions.[73] These restrictions can include (*a*) a ban on the re-export of the items to another state, (*b*) a ban on the retransfer of the items to another end-user, and (*c*) specific limitations on how, where and by whom the items can be used. States have developed templates at the EU level outlining elements that can be inserted into EUCs associated with transfers of small arms and light weapons.[74] However, there is currently no template that applies to transfers of CCICs. One national official indicated that their government is in the process of developing a new template of EUCs and EUSs for exports of dual-use items and is considering the inclusion of specific language relating to exports of CCICs.[75]

States can implement post-shipment measures to ensure that the obligations outlined in EUCs are being respected by the end-user. Post-shipment measures that are potentially relevant for transfers of CCICs include monitoring open-source media for reports of diversion, collecting information through national embassies abroad on reports of diversion, and requiring that the exporting company report suspected or confirmed cases of diversion.[76]

Good practices for applying end-use/end-user controls to transfers of CCICs

PMP code of practice supporters could adopt the following good practices:

- Adopt export licensing criteria that reflect the human rights risks associated with the use of CCICs and outline the oversight measures that recipient states need to have in place to ensure responsible end-use of CCICs.
- Use EU and PMP forums to develop joint guidelines that outline the oversight measures that recipient states need to have in place to ensure responsible end-use of CCICs. Where appropriate, include opportunities for stakeholder consultation in the process of developing such guidelines.
- Adopt decision-making processes that enable all exports of CCICs to be assessed against human rights criteria and for licences to be denied if a CCIC might be used to facilitate human rights violations.

[73] End-user certificates are issued by or on behalf of the end-user and identify, at a minimum, the material to be transferred, the destination country and the end-user. End-user statements are a form of EUC issued by private companies. See Bromley, M. and Griffiths, H., 'End-user certificates: Improving standards to prevent diversion', SIPRI Insights on Peace and Security No. 2010/3, Mar. 2010.

[74] See Council Decision (CFSP) 2021/38 of 15 January 2021 establishing a common approach on the elements of end-user certificates in the context of the export of small arms and light weapons and their ammunition, *Official Journal of the European Union*, L14, 18 Jan. 2021.

[75] Government official, Interview with the authors, 28 Nov. 2025.

[76] See Bromley, M., Héau, L. and Maletta, G., 'Post-shipment on-site inspections: Multilateral steps for debating and enabling their adoption and use', SIPRI Policy Paper, Oct. 2022.

- Ensure that the national authority has access to the expertise required to apply export controls to transfers of CCICs and to assess exports against the human rights criteria.
- Use Wassenaar, EU and PMP forums to present and discuss detailed information about how export controls are being applied to CCICs and cases where unlicensed transfers have been detected and prevented.
- Use Wassenaar and EU mechanisms to share as much information as possible about approvals and denials of export licences for the transfer of CCICs.
- Use EU and PMP forums to exchange information on the language used in EUCs and EUSs connected to transfers of CCICs and the application of post-shipment measures, and to agree on language that can be used for future exports.

PUBLISHING INFORMATION ON THE APPLICATION OF CONTROLS TO TRANSFERS OF CCICS

PMP code of practice supporters have made the following commitment relevant to publishing information on the application of controls to transfers of CCICs:

- Exploring opportunities to implement appropriate transparency around the processes implemented for controls on the export . . . of CCICs, meeting the interest of individuals and the public to be informed, and the need to prevent the disclosure of information that could impact commercial sensitivity, law enforcement, national security and defence interests, and public safety.[77]

If it is made public, the information that states collect as part of the export licensing process can act as a source of transparency, in terms of assessing how states are implementing controls on exports of CCICs and generating a more detailed picture of the global trade in these items.

Many states publish detailed information on licences issued and denied for exports of military equipment.[78] However, very few states publish equivalent information on exports of dual-use items. Two key exceptions are the UK and Switzerland, which publish data on exports of dual-use items at a level of disaggregation that makes it possible to identify licences granted and, in the case of Switzerland, licences denied.[79] The UK also regularly publishes case studies that detail the processes associated with assessing particular export licence applications.[80]

[77] British FCDO, PMP code of practice (note 2), para. 11.b.iv.

[78] See SIPRI, 'National reports on arms exports', [n.d.].

[79] See British Department for Business and Trade, 'Reports and statistics home', 15 May 2025; and Swiss State Secretariat for Economic Affairs (SECO), 'Permis d'exportation individuels établis pour les biens à double usage et de biens militaires spécifiques' [Individual export permits issued for dual-use and specific military goods], 1 Apr. 2025.

[80] See section 10 in British Export Control Joint Unit and British Department for Business and Trade, *United Kingdom Strategic Export Controls: Annual Report 2024*, 17 July 2025, pp. 51–52.

In January 2025 the EU began publishing more detailed information on export licences issued by EU member states for transfers of cyber-surveillance items.[81] Reports issued in January and July 2025 covered licences issued and denied during 2022 and 2023 for the control items listed in boxes 1 and 2.[82] For each category of item, the EU lists the number of export licence applications and the EU member states that received applications. The EU also lists the destinations that were named in at least one application, the number of export licences issued and denied, and the EU member states that issued and denied export licences. It is not possible to see which EU member state issued or denied licences for any specific destination or which categories of items were transferred to any specific destination. Moreover, only 14 EU member states provided data for the 2022 and 2023 reporting periods.

Good practices for publishing information on the application of controls to transfers of CCICs

PMP code of practice supporters could adopt the following good practices:

- Publish national data on export licences granted and denied for transfers of CCICs, including, if possible, details of each item, its destination and the type of end-user.
- Expand the EU's process of publishing information on export licences for transfers of cyber-surveillance items by adding new categories of data and encouraging all EU member states to participate.
- Use PMP forums to agree on minimum standards for the publication of data on licences for exports of CCICs that build on existing national and EU practices.

[81] European Commission, 'Comprehensive data sets related to export controls of dual-use items for the year 2022', Commission Staff Working Document, SWD(2025) 8 final/2, 5 May 2025; and European Commission, 'Statistical update on dual-use export controls—2023', Commission Staff Working Document, SWD(2025) 181 final, 4 Jul. 2025.

[82] European Commission, SWD(2025) 8 final/2 (note 81), pp. 189–195; and European Commission, SWD(2025) 181 final (note 81), pp. 160-162.

DOI: https://doi.org/10.55163/ESHD4578

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org