



Brussels, 24.1.2024
COM(2024) 24 final

WHITE PAPER
on Outbound Investments

WHITE PAPER
on Outbound Investments

1. INTRODUCTION: WHY A WHITE PAPER ON OUTBOUND INVESTMENTS?	2
2. STATE OF PLAY AND INITIAL FINDINGS	4
3. PROPOSED NEXT STEPS: REVIEW OF CERTAIN OUTBOUND INVESTMENTS	5
3.1. Proposed monitoring / review of outbound investments in specific technologies	6
3.2. Risk assessment by Member States	10
3.3. Reporting to the Commission and other Member States	10
3.4. Joint assessment and debate	11
3.5. Review of dual-use export license applications in the context of outbound investments, consultation among Member States and information to the Commission	11
4. CONCLUSION	12

1. INTRODUCTION: WHY A WHITE PAPER ON OUTBOUND INVESTMENTS?

The Joint Communication on a European Economic Security Strategy adopted on 20 June 2023¹ (‘the Joint Communication’) recognises the importance of open global markets for the success and economic security of the European Union in terms of both resilience and competitiveness. It confirms that “*our economies thrive on open and rules-based trade and investment, on secure cross-border connectivity and collaboration on research and innovation*”. At the same time, it recognises that potential security risks could arise when sensitive technologies and investments leave the EU in a way that can threaten international peace and security. In particular, it refers to the **risks of technology and know-how leakage as a result of outbound investments** (i.e., investments made by EU companies in third countries) in a narrow set of advanced technologies that could enhance military and intelligence capacities of actors who may use these capabilities to threaten international peace and security.

The EU **already restricts the export of dual-use technologies**. However, there are growing concerns that some sensitive technologies and know-how could end up in the wrong hands as a result of outbound investment transactions that are not currently subject to control mechanisms. For instance, this could happen if cutting edge EU technology reaches countries where the boundaries between civil and military activities are blurred. Such technology or know-how could be used to strengthen their military and intelligence capabilities that in turn could threaten our common EU security. Certain outbound investments can be seen as a “*reverse side*” of dual-use export transactions.

A similar **link exists between outbound investment and inbound foreign direct investment (FDI)**. The EU already has a framework to screen inbound FDI, notably, in sensitive technologies. While an inbound investment into EU companies holding sensitive technologies by risky investors could be restricted or prohibited by measures imposed under an FDI screening regime, there is a potential risk that the targeted EU companies could make those technologies available to the same investors by means of outbound investments. However, such outbound investments are currently not even subject to monitoring. This could undermine the effectiveness of our existing controls and, hence, security of the EU as a whole and of individual Member States.

Such growing concerns underline the **need to look at this issue closely** to understand:

1. **What kind of investments** in certain critical technologies are made from the EU;
2. **Whether** such investments may effectively put EU or Member State security at risk; and, if so,
3. **To what extent** such risks can be mitigated by existing tools or would justify additional proportionate policy action at EU or national level.

¹ Joint Communication to the European Parliament, the European Council and the Council an “European Economic Security Strategy”, Brussels, 20.6.2023, JOIN(2023) 20 final.

From a geostrategic perspective, the EU is not the first to consider a policy initiative in this area. **Some countries already control outbound investments**, such as Japan² or China³. Others, like the United States⁴, are developing a framework to do so.

Developing an EU response to concerns regarding outbound investments presents a number of challenges: (i) determine the scope of potential concerns, (ii) understand the extent and nature of EU outbound investments by collecting relevant data and evidence, and (iii) assess whether such investments create or aggravate clearly identifiable risks to security. In a second step, the EU and its Member States should assess the need for proportionate and targeted responses to mitigate identified risks either through existing tools or new mitigating action at national and / or EU level.

A comprehensive assessment requires a good understanding of outbound investments by EU investors and of the technology and know-how that may be transferred in the context of such transactions. It also requires an in-depth understanding of security risks related to such outbound investments in order to assess potential gaps in existing trade and investment security tools.

The present White Paper describes the state of play of the EU's initial work on outbound investment. It outlines a way forward to understanding and addressing current challenges with a uniform and effective EU approach. Its aim is to invite comments and input from interested stakeholders in order to help the Commission define the scope of a future Commission Recommendation on outbound investment in close cooperation with Member States. The High Representative / Vice-President (HRVP) may provide his input, where appropriate, in relation to possible issues concerning common foreign and security policy. This White Paper will help the Commission to understand the views and concerns of stakeholders and of the European Parliament while keeping in step with the ongoing reflections and analyses within the EU⁵ and Member States on the issue of outbound investment and economic security in general.

² Pursuant to certain conditions established by the “[Foreign Exchange and Foreign Trade Act \(Act No. 228 of 1949\)](#)”. The Japanese outbound investment controls apply to investments in very few sectors: fisheries, leather and leather products, weapons and weapons equipment manufacturing, and narcotic drugs.

³ In China, existing legislation includes the “[Administrative Measures for Overseas Investment by Enterprises, by the National Development and Reform Commission \(2017, No. 11\)](#)”, the “[State Council Guidance on Overseas Investments \(2017, No. 74\)](#)”, which identifies *encouraged*, *restricted* and *prohibited* outbound investments, and the “[Catalogue of Sensitive Industries for Overseas Investments, by the National Development and Reform Commission \(2018, No. 251\)](#)” which lays out the sensitive industry sectors for overseas investments. These include weapons and related equipment, water resources, news media, real estate, hotel, cinema, entertainment industry, sports clubs and certain equity investment funds. We understand that the various Chinese licensing and registration requirements related to outbound investments not only serve the interests of national security and foreign trade control, but also the broader “*national interest*”. China also restricts foreign currency exports under the State Administration of Foreign Exchange. Thus, it appears that the Chinese outbound investment controls cover a wide set of economic sectors and a substantive test that goes potentially beyond a pure security assessment.

⁴ [Executive Order 14105 of August 9, 2023, Advance notice of proposed rulemaking of 14 August 2023.](#)

⁵ Including the separate, but to some extent related, risk assessment on the four prioritised critical technologies following the Commission Recommendation C(2023) 6689 final of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States.

2. STATE OF PLAY AND INITIAL FINDINGS

Ahead of the Joint Communication, the Commission launched a debate on this issue with FDI screening and dual-use export control authorities of Member States in the spring of 2023. To feed this debate, the Commission has been **gathering data** on outbound investments by EU companies. In the period from 2013 to 2022, there have been around 12.800 Merger and Acquisitions transactions by EU companies in third countries corresponding to roughly EUR 1.4 trillion and 26.000 Venture Capital investment transactions with an overall value of EUR 408 million.⁶ For both categories of outbound investment transactions, the top two destinations were the USA and the United Kingdom, which represented at least half the deals and approximately 70 % of the capital. Beyond these high-level information, the Commission has found some significant limitations in the available data, such as further details on the transactions, monetary amounts, deal characteristics, technologies involved.

On the one hand, official sources (e.g., FDI data from national accounts) lack updated and detailed data on the sector or technology related to individual investment transactions, making it challenging to identify those outbound investments in a narrow set of critical technologies where potential risks might arise. On the other hand, official statistics as well as available commercial data sources, classify companies and transactions according to official classification systems. These mostly describe areas of already developed technologies, but do not provide information on specific advanced technologies or new economic activities, such as artificial intelligence.

Last July, the Commission set up an **Expert Group on Outbound Investment** ('the Expert Group'), aimed at drawing in knowledge and experience from Member States in order to examine potential security risks, gaps, and, if needed, possible policy actions.⁷ The Expert Group brings together Member States' experts from dual-use export controls, FDI screening, trade and foreign affairs departments. It has already met three times in 2023.

By now, it has become clear that before analysing any possible risks, there needs to be a clear understanding on the **scope of the exercise** – effectively, "*which outbound investments should be considered to identify risks for our common EU security*" – and that **concrete granular data** at national level **on relevant outbound investment transactions** and, possibly, on related activities **is needed, but is currently missing. This lack of data shows a need to build a shared view on the scope of the issue**, as regards the scope of transactions and activities leading to risks, the technologies potentially concerned and on whether the focus should be on specific countries.

⁶ Source: Pitchbook data extracted in July 2023. Notes: (1) the data cover only M&A deals and VC investments, as greenfield investments are not included in the consulted commercial database(s); (2) the monetary amount for M&A deals is incomplete as values were only available for half of the deals; and (3) VC transactions are counted where at least one EU investor was involved, but it could be part of a group of non-EU investors and the total amount invested is the one reported, without further identification of the amount(s) of the relevant EU investments.

⁷ [Register of Commission expert groups and other similar entities \(europa.eu\)](https://ec.europa.eu/euipo/commitment/commitment-2023-07-14).

The ongoing work with Member States in the Expert Group has led the Commission to the following initial findings:

1. **There is a substantial knowledge gap** and a very limited picture of the outbound investments made by EU investors. Some public authorities are gathering information at national level (e.g., central banks or national statistical offices⁸). This information is, however, neither sufficiently granular, nor targeted enough to provide the relevant facts to establish whether any security risks can arise from these investments and to allow Member States and the Commission to carry out a proper assessment of such risks.
2. **Member States do not systematically review and assess outbound investments for security purposes.** Several Member States acknowledge the possibility that, as a result, some risks are being overlooked.
3. **The matter is both sensitive and complex.** While potential risks stemming from certain outbound investments have a broader geopolitical dimension, it is important to recognise that EU outbound investments are a valuable and legitimate part of economic activity in a global market place. Therefore, any potential policy action concerning outbound investments may come with positive and negative implications for EU businesses.
4. There is consensus among Member States and the Commission that, should any risk be identified, **policy action should be effective, proportionate, targeted, and enforceable** by administrations.
5. **Before designing any new policy responses, we need to make full use of existing instruments first.** In case policy action will be deemed necessary to respond to identified risks, the Commission and Member States should try, to the extent legally possible, to address any risks from outbound investments through existing instruments, such as dual-use export controls or FDI screening mechanisms, either by enhancing the use of these instruments or by amending them to cater for new risks.

3. PROPOSED NEXT STEPS: REVIEW OF CERTAIN OUTBOUND INVESTMENTS

This is a complex matter which deserves a **gradual step-by-step approach**:

- first, a public consultation stage: launched by the publication of this White Paper and a questionnaire;
- second, a monitoring stage: the Commission will draw on the the results of the upcoming public consultation and the reactions to this White Paper to draft a

⁸ Some **legislation allows Member States to (partially) monitor outbound investment** transactions, like balance of payment statistics gathered by Central Banks, national registries aimed at monitoring outbound investments for statistical purposes and similar legislation, e.g., Spain's national regime established by Royal Decree 1265/1986 of 27 June 1986, Chapter VI, updated with Royal Decree 664/1999 of 23 April 1999 and with Royal Decree 571/2023 of 4 July 2023. **Further information may be gathered through official investment guarantee schemes**, e.g., the investment guarantee schemes of Germany and Austria. In Germany this is managed by PwC on behalf of the Federal Ministry for Economic Affairs and Climate Action, while in Austria it is managed by a bank (OeKB) on behalf of the Federal Ministry of Finance. **Some national mechanisms enable Member States to control very specific instances of outbound investments** for security purposes (e.g., Italy's Golden Power regime, pursuant to Law Decree No. 21/2012, which contains some provisions allowing the screening of limited types of outbound investments).

Recommendation to Member States to monitor/review certain outbound investment transactions involving a set of sensitive technologies over a certain period of time;

- third, a risk assessment stage: on the basis of the results of this analysis and monitoring, the Member States and the Commission will be in a better position to draw conclusions regarding the risks linked to such outbound investment transactions for our common EU security.

The results of that assessment and possible proposals to mitigate any identified risks will be set out in a further Communication and, as necessary, any appropriate proposals.

3.1. Proposed monitoring / review of outbound investments in specific technologies

Based on the initial findings from the work undertaken with the Expert Group, the Commission invites comments on the aspects set out below that will be addressed in the proposed Commission recommendation on monitoring.

Scope of monitoring

1. Regarding the type of outbound investment transactions to be monitored, the Commission considers that the **monitoring should cover a wide range of transactions**, including all kinds of active investments, while excluding portfolio investments, i.e. non-direct foreign investment with the purpose of making a financial investment without any intention to influence the management and control of an undertaking, as set out in the box below.

Member States should monitor investments of any kind by natural or legal persons resident or established in the EU ('EU investors') aimed at carrying out an economic activity outside the EU. Such investments should include:

- the acquisition of a company or a stake in a company that enables an effective participation in the management or control of the company ('acquisition'),
- the absorption by one company of one or more other companies or the combination of two or more companies to form a new company ('merger'),
- the transfer of tangible or intangible assets, including intellectual property or specific know-how and technology process, necessary for establishing or maintaining an economic activity ('asset transfer'),
- the first-time establishment of a business, including the creation of a subsidiary, a branch or similar ventures ('greenfield investment'),
- the establishment of a venture to combine resources to achieve a joint entrepreneurial goal with another person ('joint venture'), and
- the provision of capital to develop a sensitive technology, linked to certain intangible benefits like managerial assistance, access to investment and talent networks, market access and enhanced access to additional financing ('venture capital').

The monitoring should also cover other (indirect) investments made by an EU investor, such as investments made through a third-country entity which is used as an investment vehicle, through an existing subsidiary or in the context of an existing joint venture. This includes the gradual transfer of assets over time, investments in third countries that result from previous investments and investments aimed at circumventing existing security-related trade and investment controls. The monitoring should exclude portfolio investments.

Further on the scope, the Commission invites comments also on risk-based priorities that might be established within the monitoring, such as those routinely used by Member States' export control authorities in their assessments of dual-use export licence applications. This could include prioritising monitoring on the basis of the profile of the end user and its country of establishment.

2. In addition, in light of the input received from the Expert Group, there are concerns that limiting any assessment just to the type of activities covered in point 1 above may not capture potentially risky activity linked to or preparatory to such outbound investments. The Commission therefore also invites comments on whether it should recommend that **Member States may also decide to monitor other critical activities** ('optional monitoring'), such as **research and development cooperation**, or practices used to **attract highly specialised personnel** in order to benefit from their know-how and experience in certain sensitive areas, or to get access to intellectual property, as set out in the box below.

Member States could consider monitoring the following activities, which may also lead to a risk of the leakage of sensitive technology or know-how:

- **Research cooperation**, which is to be understood as cooperation between an entity established in the EU and an entity established in a third country related to the transfer of tangible or intangible assets in the four critical technology areas as set out in section 3 below, including intellectual property and know-how. This could include cooperation between entities such as research and academic institutions, or between these institutions and private or public sector entities. This optional monitoring is to be seen in light of existing or upcoming Member States' efforts to develop an approach for enhancing research security, also in line with the Proposal for a Council Recommendation on enhancing research security adopted by the Commission on 24 January 2024.⁹
- **Mobility and transfer of highly specialised personnel**, including specialists in the four critical technology areas, or business executives with significant experience in the four critical technology areas.

3. Regarding the technology areas in which investments should be monitored, comments are invited on whether **monitoring should initially focus on the most sensitive technology and know-how**. This could, for example, cover four technology areas: advanced semiconductors, artificial intelligence, quantum technologies and biotechnologies. These represent technology areas identified by the Commission as **"highly likely to present the most sensitive and immediate risks related to technology security and technology leakage"** in the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States of 3 October 2023¹⁰. Under that Recommendation, a risk assessment on these technology areas is currently being undertaken by the Commission

⁹ Proposal for a Council Recommendation on enhancing research security COM(2024) 26 of 24.1.2024.

¹⁰ C(2023) 6689 final.

and Member States. It is of a broader nature covering a range of risks linked to these particular technologies. It includes an initial view on the potential for technology leakage linked to outbound investments. The outcome could be used as an input for the more in-depth assessment of risks related to outbound investments to be performed by Member States and the Commission on the basis of the proposed monitoring. The results of this on-going assessment of critical technologies as well as reactions to this White Paper could, for example, confirm or lead to changes in the scope of the technologies that the Commission may recommend Member States to monitor.

4. With regard to the **geographical coverage**, the work of the Expert Group suggests that both the Commission and the Member States share the view that monitoring should not a priori exclude specific destinations. Nevertheless, in light of the high number of countries and existing resource constraints, the Commission is of the opinion, that **Member States should best prioritise their monitoring activities based on their assessment of the risk profiles of certain countries**. The risk assessment should include the past behaviour of the country concerned, including violations of the UN Charter. This risk profile should also assess the possibility of technologies or items to be used in war or conflict situations, for breaches of human rights or to enable the proliferation of weapons of mass destruction, in full respect of the obligations and commitments taken by Member States or the EU as members of international non-proliferation agreements and multilateral export control regimes.

Time Period covered and Information to be collected

5. With regard to the **time period covered**, in order to develop a sufficient basis to identify and assess the level of outbound activity and associated risks within a reasonable period of time, the Commission considers that the monitoring should cover both new and ongoing transactions and certain past transactions. This should involve Member States assessing **transactions** in the selected technology areas **completed since 1 January 2019**. Comments are also invited on this suggested time period.
6. With regard to **information to be gathered**, the proposed monitoring should **provide Member States and the Commission with the necessary data and information in order to assess risks linked to outbound investments** in the selected technology areas. This data and information should be shared with other Member States and the Commission through the Expert Group. The Commission invites comments on the information to be gathered as set out in the box below.

The monitoring should enable Member States to gather all necessary information for the risk assessment, including as minimum:

- Information on the parties to the investment transaction, including the full place of incorporation of legal persons and (based on the best information available to the Member State) the ultimate owner(s) of any parties involved in the transaction,
- the type and approximate value of the investment,
- the products, services and business operations related to critical technologies concerned by the investment,
- the date on which the investment is planned to be completed or has been completed,

- based on the best information available to the Member State, information about previous and planned or contemplated future transactions entered into by the parties to the investment transaction.

Regarding other related activities, that could be subject to the optional monitoring, this information could at a minimum include:

- information on the persons involved in the activity, including the full name, address and nationality of natural persons or the registered address and place of incorporation of legal persons,
- based on the best information available to the Member State, an exact description of the activity,
- the critical technologies concerned by the activity,
- the date on which the activity has commenced, is foreseen to commence, or has ended,
- based on the best information available to the Member State, information about previous and planned or contemplated future activities undertaken by the same persons involved in a current activity.

Any data collected should be protected appropriately and, where necessary, classified before being shared with other Member States and the Commission.

Other aspects of monitoring: who is responsible at a national level, what tools should be used and how will Member States ensure stakeholder involvement?

7. In order to ensure that monitoring work can be taken forward, the Commission is of the opinion that Member States should **designate an authority responsible for the monitoring** and should ensure that the competent national authorities, where possible, apply existing instruments, including dual-use export controls, to counter any risks they have identified in the monitoring to be recommended.
8. **Monitoring tools and exchange with stakeholders:** for the monitoring process to be effective, Member States will need to ensure that they have adequate monitoring tools and sources of information, and if this is not the case, they should consider adapting existing tools or put new ones in place for the purpose of the proposed monitoring activities set out above.

Existing **monitoring and other tools that could be used or adapted** for this purpose include **reporting obligations to central banks or national statistical offices** and similar institutions for statistical and balance of payment purposes, notification requirements to national export control authorities for the export, brokering, technical assistance, transit and transfer of dual-use items as well as any investment transactions. Member States should also consider official investment guarantee schemes or official export credits schemes as a source of relevant data. Any data collected should be protected appropriately and, if appropriate, classified before being shared with other Member States and the Commission.

Comments are invited on the tools that might be needed for effective monitoring, their feasibility and the balance to be struck in terms of the burden that such information collection may represent and the need to ensure a sufficient basis to monitor and assess

outbound activity and risks in the sectors selected. In addition, the Commission considers it will be important for Member States to consult relevant stakeholders, including business, academia and civil society as part of their monitoring activity.

3.2. Risk assessment by Member States

Drawing on the results of the proposed monitoring, the Commission considers that Member States should perform the following initial risk assessment to identify either the presence or the absence of risks to security. The assessment should be based on the information gathered by monitoring outbound investments, and possible additional activities that they choose to monitor, as specified above.

To structure the risk assessment, the Commission believes that the following elements could guide the assessment by Member States.

- The assessment should be as comprehensive as possible. Work should give priority to those transactions or activities which would present a risk for the security of the EU as a whole and it should also try to assess the degree of likelihood that any negative impact materialises.
- The assessment should identify elements of risks and potential vulnerabilities such as the main types of threats and threat actors and any relevant geopolitical factors.
- The assessment should take into account, inter alia, the context of the transaction, the value chain and supply chain of the technology involved, the evolution of risks as well as relevant technological developments, and the global interconnectivity of the ecosystem of the critical technology concerned, including research activities.
- Member States could consider following similar methodologies to those used in reviewing dual-use export licence applications and for screening foreign direct investment transactions.

This risk assessment should enable each Member State to identify and analyse vulnerabilities that may have a potential impact on the security of the EU as a whole or on Member States' security, and the likelihood of a related adverse impact materialising. The elements above to frame the risk assessment will be further developed in the future Commission Recommendation taking into account the ongoing work in the Expert Group with Member States, the results of the public consultation and the reactions to this White Paper, with a view to develop a common methodology. This will ensure a consistent and EU-wide risk assessment from all the Member States. Where possible, Member States and the Commission should look for synergies between different assessments of security risks under the framework of the Joint Communication.

3.3. Reporting to the Commission and other Member States

Time will be needed for Member States to establish monitoring of new and on-going transactions and to assess on the basis of available information what has happened since 2019. The Commission therefore proposes that Member States conduct this monitoring within a 12 month-period from the adoption of a Commission Recommendation. This period, combined with the initial consultation stage up to summer 2024, should allow them to put such a monitoring system in place and carry out their initial assessment. During this time, Member States and the Commission would continue exchanging information and views in the

framework of the Expert Group to ensure that, to the extent feasible, the monitoring and risk assessment follow a common methodology.

Member States should report to the Commission and other Member States on the outcome of the monitoring and the outcome of their analysis and risk assessment. If risks related to a combination of certain factors or patterns that characterise any types of outbound investments likely to affect EU or Member States' security are identified, Member States should provide the Commission with the combinations of risk factors and describe these patterns.

3.4. Joint assessment and debate

The Commission proposes that the outcome of the monitoring and risk assessment to be undertaken by Member States is to be shared with the Commission and the other Member States, in accordance with the appropriate classification level. Based on the shared input, **the Expert Group would discuss the outcome of the monitoring and risk assessment** with a view to consolidate the overall results and help the Commission prepare a final comprehensive risk assessment and **ensure a shared understanding of risks**. Other stakeholders may be also consulted at this stage, as appropriate.

This will be a useful **reference point for any debate on further policy choices** and the possible need for mitigating measures or other policy responses.

3.5. Review of dual-use export license applications in the context of outbound investments, consultation among Member States and information to the Commission

In parallel to the proposed monitoring and review, in light of the close links explained in Section 1 above between dual-use export controls and outbound investments, the Commission is of the opinion that Member States, when reviewing licence applications for exports of dual-use items, should pay particular attention where such applications are linked to outbound investments, and any risks these may present. This could offer useful insights for the monitoring work.

Since priority should be given to the use of existing instruments, the Commission considers that Member States should in such cases give particular consideration to applying existing instruments to address potential concerns when relevant, including “catch-all”¹¹ export controls, to mitigate the risks of such technology contributing to destabilising military application, proliferation of chemical, biological or nuclear weapons, or human rights violation, that could create a threat to international and regional peace and security.

To the extent legally possible, the Commission invites Member States' export control authorities to consider consulting with other Member States and informing the Commission, when reviewing dual-use export licence applications in the context of outbound investments in

¹¹ “Catch-all” controls are generally understood to be controls that are applied by Member States to items that are not listed in Annex I to Regulation (EU) 2021/821 (the “Dual-Use Regulation”), the so called ‘EU control list’, so the controls apply to items that have not yet been agreed under the multilateral control regimes. Most notably, Article 4 of the Dual-Use Regulation requires exporters to seek an export authorisation if they are informed by the competent Member State authority that an item that they export may be intended for one of certain sensitive end-uses detailed in Article 4. Such information generally takes the form of a non-public individual notification to the relevant exporter.

the four critical technology areas, which are likely to have an impact on the security of other Member States. This consultation could be done informally and modelled on the cooperation mechanism established for foreign direct investment screening under Regulation (EU) 2019/452.

Within the same deadline as the monitoring exercise, the Commission proposes that Member States report to the Commission and to other Member States on the implementation of export controls in this context, including on the number and content of licence applications received for exports taking place specifically in the context of an outbound investment. During this period, Member States and the Commission will continue exchanging information and views on these matters in the framework of the Expert Group.

4. CONCLUSION

This White Paper maps out the first policy initiative, which the Commission takes in the field of outbound investments. Recognising its complex and sensitive nature, the Commission proposes a gradual approach, working closely with the Member States' authorities through the Expert Group on Outbound Investment

In order to structure responses to the ideas set out in this White Paper, the Commission is launching a public consultation based on a detailed questionnaire that stakeholders, including business, academia and civil society are invited to fill out.

It will only be possible **to design adequate responses to protect the security of the EU and its Member States on the basis of comprehensive assessments**. In shaping such responses, priority should be given to making full use of existing instruments rather than establishing new ones. Any **responses should be proportionate, precisely targeted and enforceable** to address the risks identified for each type of outbound investment or activity and critical technology area.

Work in the Expert Group on Outbound investment will continue in 2024 together with the consultation of stakeholders. The Commission will also seek the views of the European Parliament and like-minded partner countries.

Timewise, the next steps are therefore the following:

- January 2024: adoption of the White Paper on outbound investments;
- January – April 2024: public consultation on the proposed monitoring and review of certain existing outbound investments and related activities;
- Summer 2024: assessment of the results of the consultation and adoption of a Commission Recommendation to Member States to launch the proposed monitoring and review;
- Summer 2025: conclusion of the proposed monitoring and review by Member States and risk assessments of outbound investment transactions;
- Autumn 2025: Assessment by the Commission of the need and possible content of policy responses in this field.

*

*