EECARO
European Export Control Association
for Research Organisations

22 December 2023

Feedback on the Call for Evidence on enhancing research security in Europe

EECARO welcomes the stakeholder consultation in preparation of the Commission proposal for a Council Recommendation on boosting research security in the European Union. It is understood that this Recommendation as soft law is not the endpoint, but a step in the dialogue between policymakers, government administrators and research organisations to seek alignment as much as possible in the ensuing process.

EECARO, established to unite research organisations in dealing with challenges related to export controls, recognizes the multifaceted nature of the concept of research security, and is particularly interested in its dimension of undesirable transfer of higher risk technology (for military or Weapons of Mass Destruction use, for loss of technological innovation lead, or for human rights concerns). This dimension is linked to the aspects of technology security and technology leakage in the recent EU policy priority of economic security and in the knowledge security policy under development by (at least) the Netherlands. EECARO therefore focuses its initial feedback, grouped into the 8 points below, to the intersection between export controls, research security, economic security and knowledge security.

1. EECARO emphasizes the **importance of open science, academic freedom, and international collaboration without unduly restrictions**. Restrictions should be possible, but only where and to the extent that they are indeed necessary to safeguard from the undesirable transfer of high-risk technology to non-state and state actors of concern. Imposing restrictions beyond what is needed to mitigate risks linked to specific technologies and to specific security risks, is likely to (further) create complexity and uncertainty for research activities and collaborations. This is especially the case in the context of globalised and interconnected research networks and platforms, where the boundaries and definitions of what constitutes a collaboration of concern are unclear, ambiguous, or inconsistent.
2. EECARO favours a **balanced and proportionate approach to research security, adopting a risk-based assessment and management of security risks.** This means applying new and existing regulatory instruments such as export controls, (inbound and outbound) investment screening, knowledge security and economic security only to research collaborations and output that pose a significant risk to or impact on national security, including technology leakage, and that are not widely available or accessible to the public or the research community. A risk-based approach also entails assessing and mitigating the potential downsides of such regulatory instruments on research activities and collaborations, such as loss of competitiveness, innovation, or reputation. Export controls can serve as an inspiration to research security for their systematic transaction-based approach for listed technologies complemented with a case-specific approach for

end-uses or end-users of concern. Export controls, however, have also proven the difficulties in linking emerging technologies research with controlled performance levels, characteristics, or functions. Another critical nexus between research security and export controls is present in procurement, contracting, and human resources policies. Identifying associated risks prompts the need for appropriate measures, for instance relating to screening assessments to be conducted during the recruitment and selection process. Hence, the practices and principles required for compliance in both the export controls and research security domains may intersect and sometimes create positive or negative interference. This underscores the importance of harmonising the approaches to ensure a cohesive and effective framework in managing these interconnected aspects.

3. EECARO strongly supports **the emphasis on institutional autonomy and self-governance balanced with clear regulatory requirements and guidance**. EECARO understands that the scale and depth of regulatory measurements and requirements for research organisations is still under development in a challenging geopolitical climate. But the EU-level policy aspiration to remain fully country-agnostic to avoid discrimination and stigmatisation leaves research organisations and EU Member States at risk to tackle similar technology security and leakage risks in an uncoordinated way. EECARO sees more added value in a balanced approach between general purpose research security regulatory requirements or guidance on the one hand, and targeted requirements or guidance to the highest-risk technologies, and in some circumstances to specific (non-) state actors of concern, on the other hand.
4. Ensuring a **level-playing field within the EU (and between the EU and like-minded partners)** requires the reduction of disparities in (national) research security measures as much as possible, and the necessity to harmonise incentives and enforcement. By means of example, EECARO refers to the national export controls recently adopted by Spain and the Netherlands (and in preparation by Finland), and the Netherlands notably introducing the concept and practice of knowledge security. Such proliferation of measures puts further tension to the due diligence efforts of research organisation across different countries. The uneven level-playing field is also exemplified by the U.S. exemption regarding the intention to publish or diverging definitions of fundamental research in the area of export controls.
5. Within Member States, EECARO observes a **proliferation of requirements and concepts connected to the notion of security and dual-use**. EECARO strongly favours a Recommendation on the notion of research security that does not contribute to further complicating the notion of dual-use research or technologies. EECARO highlights the current mismatch in expectations for research organisations between the regulatory instruments of research funding and export controls in the context of international collaboration on dual-use technologies.
6. EECARO sees benefits **to support established associations in developing and maintaining a research security training and education program** for their members. Such a program can provide and deliver the necessary knowledge and skills to (new) researchers and research organisations, and it raises and maintains the awareness and culture of research security in an evolving regulatory and geopolitical landscape.
7. EECARO remarks that the current 'de-risking' policy rhetoric (without clear regulation or guidance) puts **significant due diligence challenges for research organisations**. Legal

and reputational risks, and liabilities for non-compliance or violations require substantial resources and capacities for research organisations to implement and comply with the ever-increasing proliferation of regulatory instruments. This approach needs to be accompanied with an increased effort from regulators to provide adequate tools and a contact point for research organisations to get effective and timely feedback on questions related to the implementation of research security. Addressing requirements and aspirations linked to export controls, foreign interference, research security, knowledge security, and (inbound or outbound) investment screening requires a coordinated approach within research organisations. This task becomes even more challenging when the risk assessment or management is fragmented across different dedicated committees and appointed staff. This fragmentation then risks overlooking the overall strategic challenges involved in specific research or collaborations and may result in inefficiencies.

8. EECARO advocates that the **Council Recommendation**, while not legally binding, should be persuasive and authoritative so that it reaches the policy objectives assigned to it. It should be adequately comprehensive and detailed so that it fosters practical value in implementation. Existing documentation on the topic, such as the staff working document on 'Tackling Research and Innovation Foreign Interference', provides a good starting point in setting the scene and raising awareness, but the Council Recommendation should aim higher and describe the roadmap for activities that are considered best practices for the European research organisations when ascertaining research security in their activities. In drafting the Council Recommendation, it may be productive to investigate which practices currently employed in the European research organisations could be considered best practices and, consequently, be recommended by the Council. This approach would serve the interests of increasing efficacy of the Council Recommendation and achieving the needed level-playing field among the European research organisations.

To conclude, EECARO sees the following **key strategies and actions for enhancing research security awareness and management**:

- promote research security as a shared responsibility and a core value. This means communicating and demonstrating the importance and benefits of research security for the research community and society. This also means countering unfair Research and Innovation via multilateral dialogue.
- provide research security guidance and support. This means offering and facilitating the access to and use of research security resources, such as information, advice, and tools, which enable and assist the research organisations and regulators in implementing and complying with research security policies, standards, and procedures. It should be avoided to mix general purpose risk mitigation measures with technology specific risk mitigation measures. This will improve the quality and impact of research security activities and initiatives, and it will reduce the costs and risks of due diligence activities by research organisations.
- recognise and reward research security excellence. This means acknowledging the achievements and contributions of research organisations, and incentivising

and stimulating the improvement and advancement of research security practices and solutions. This also involves the consideration of developing benefits to research organisations implementing an effective internal research security compliance programme, for instance in seeking research funding in higher risk technology areas.

- strengthen research security resilience and adaptability. This means increasing the ability and readiness of research organisations to cope with and recover from research security incidents, and to adjust and respond to the changing and emerging research security issues and challenges, by building and maintaining trust, confidence, and cooperation, and by fostering and enabling the uptake and innovation of research security practices and solutions.

About EECARO

The European Export Control Association for Research Organisations (EECARO) is a network that aims to unite European research institutes, universities, and their export control compliance officers with a view to address the specific character of export controls in a research context. For more information, please visit: http://www.eecaro.eu | Contact: info@eecaro.eu