cnrs	**Call for evidence** **Boosting Research Security in the EU** *Contribution of the Centre National de la Recherche Scientifique*	January 2024

As pointed out by the European Union on June 20, 2023, Research Security is an essential link in the approach aiming at strengthening European economic security. Protecting research, beyond economic interests, also means protecting our common European values: « *Si nous ne portons pas au niveau français et européen cette recherche, on décide stratégiquement de dépendre de ceux qui la feront. (…) nous ne pouvons pas mésestimer le fait que nous sommes dans un monde qui se refracture et où il y a derrière des choix géopolitiques qui iront avec des choix de recherche* » [1] (quote of the French President E. Macron, November 26, 2019 on the occasion of the 80th anniversary of CNRS). As a multidisciplinary basic research organization serving society, **CNRS supports the European Research Security initiative.**

CNRS is particularly concerned by this initiative for essentially two reasons: our institution stands as a major stakeholder of European research (it is the largest employer of researchers in Europe and has been standing as the number one beneficiary of European framework programs for research and innovation for nearly 40 years). CNRS is also a long-standing operator of the French policy called "Protection of the scientific and technical potential" - Protection du Potentiel Scientifique et Technique (PPST).

CNRS therefore wishes to play an active role in the deployment of European Research Security, beyond the present participation to the Call for Evidence. Given the short time to provide feedback, the present paper can only focus on a few key highlights.

1. Operating the French system of Protection of the scientific and technical potential at CNRS

In France, a national regulatory framework has been in place since 2012 to protect scientific work (both public and private) from foreign interference, undue collection of knowledge or misappropriation of knowledge for unwanted purposes. According to Article 410-1 of the French Penal Code, the scientific and technical potential is viewed as part of the nation's **fundamental interests**. As such, it is protected by the PPST regulation - Protection du Potentiel Scientifique et Technique.
The French PPST is a **strong legal protection** based on the identification of strategic knowledge and know-how. It also targets the protection of sensitive technologies through restrictive measures, such as **Restrictive Regime Zones** (Zones à Régime Restrictif, ZRR). Through a strict access control, ZRRs are **spaces of trust** within which performed research can be securely shared. All individuals must be duly authorized to be able to work in ZRRs: the condition applies to everyone, **regardless of nationality**.

The identification of sensitive work is based on the analysis of **four risk criteria** pertaining to undue collection of knowledge, misappropriation of knowledge or foreign interference:

- Risk of affecting the economic interests of the nation. Note that in the case of public research, this potential is also understood as a risk of undermining the scientific outreach of the nation;
- Risk of strengthening foreign military arsenals or weakening the defense capabilities of the nation;
- Risk of contributing to the proliferation of weapons of mass destruction and their means of delivery;
- Risk of use for terrorist purposes, both domestically and abroad.

As suggested by these four criteria, the PPST policy also stands as a tool for compliance with other legal provisions (export of war material, dual-use goods, international treaties, etc.). Independently of ZRR's, the PPST policy applies to a variety of research contexts: recruitment, international cooperation, mobility schemes, *etc.*

[1] Translation: "If we don't support this research at the French and European levels, we are strategically deciding to depend on those who will do it. (...) we cannot underestimate the fact that we are in a world that is refracturing and wherever geopolitical choices are to be made, they will go hand in hand with research choices"

The implementation of the PPST policy is highly **centralized** and relies on a chain of players. Firstly, the PPST policy is steered and coordinated at the inter-ministerial level by the General Secretariat for National Defense and Security (SGDSN - a department of the French Prime Minister). The SGDSN has an officer in each ministry, so-called Senior Defense and Security Officers (HFDS – Haut fonctionnaire de défense et de sécurité). Each ministerial HFDS has as many representatives as there are concerned institutions. For instance, the HFDS of the French Ministry of Higher Education and Research relies on a network of Security and Defense Officers (FSD – Fonctionnaire de sécurité et de défense): each higher education and/or research institution (universities, national research organizations) has an FSD.

FSDs are responsible for the implementation of the PPST regulation in their respective institutions. As such, they are natural contact points of researchers for any question related to PPST purposes.

The approach followed at CNRS is based on four main principles:
- trust in researchers;
- acceptance from researchers;
- awareness of researchers;
- pragmatism of protection measures.

2. Comments on the Initiative recommandations

2.1. *Guiding Principles*

➞ "*Emphasis on self-governance by the sector in full respect of academic freedom and institutional autonomy*"

Protecting research from foreign interference is a matter of national interest from Member States. The R&I sector should take up Research Security at the European level, but **this principle of self-governance should also comply with existing or to-be national regulations**. This does not preclude the development and adoption of a common European base of measures to protect research and innovation.

CNRS would like to draw the attention on the legal protection of researchers induced by a national legislation. Research Security is a risk management approach and as successful as it can be, there will always be a residual risk of undue collection or misappropriation of knowledge for malicious purposes. In the event of an established incident, a French researcher who has complied with the existing regulations will not be held accountable. In France, prejudice against the fundamental interests of the nation (including scientific potential) is entitled to punishment under articles 410-1 to 414-9 of the Penal Code. Under the PPST regulation, Research institutions and ministries are liable for the most sensitive decisions. Transferring liability to researchers can lead to self-censorship, like applying a precautionary principle too systematically and too widely (e.g.: cease of all collaborations with a given country).

➞ "*Taking an all-of-government framework towards supporting and empowering the sector, notably by linking R&I and security expertise*"

More generally, balancing the benefits and risks of potential international collaborations requires a wide approach as pros and cons may be appreciated differently by different players (research stakeholders, foreign affairs, defense, economy, etc.). An **inter-ministerial (or inter Directorates General) approach** may prevail: protecting research sometimes goes beyond the competence of a single sector or a single ministry (or DG).

Once a multilateral framework has been established, the Research Security policy can then be implemented across all departments involved in research and innovation, while **maintaining dialogues** between the different stakeholders: research, innovation, security, visa issuance etc.

➞ "*Supporting an all-of-sector approach, including basic and applied research as well as higher education*"

CNRS wishes to stress that basic and applied research shall be conceived as a continuum. Hence, security concerns must cover the whole spectrum of research and innovation, taking into account the specificities and challenges associated with each TRL level.

➞ "*Proportionality of safeguarding measures based on a risk-based approach*"

Protective measures must be implemented under the principle of proportionality with the identified risks. **This assumes that risk assessment criteria be clearly established and shared by all**. It also assumes consensus on the definition of what is considered as a low, medium or high protection measure.
In order to guarantee the notion of proportionality, some flexibility should be left to national authorities for the appreciation of cases.
Additionally, an approach based on the sole risk notion (so-called "risk-based approach") may prove too narrow: risks are estimated with respect to opportunities/benefits. Hence a "**benefit/risk-based approach**" appears more appropriate.

➞ "*Focus on national security risks as well as ethics and integrity considerations*"

If national security issues are of paramount importance, the largest common denominator among EU shared values should prevail, while in the same time respecting the specific national security requirements of each Member State.

CNRS wishes to stress that reaching a common definition of the **core values to be shared** is crucial. Without an EU collective momentum for Research Security, opportunities for malicious entities to bypass national systems will remain: avoiding a European "weak link" that may serve as a "back door" for undue influence on European research should be a priority.

➞ "*Taking a country-agnostic approach avoiding all forms of discrimination and stigmatisation*"

Protective measures taken within the Research Security initiative should apply to everyone, under an erga omnes basis: they should apply to nationals, EU nationals, as well as non-EU nationals.

It is also implicit that elaborating a European Research Security policy aims at protecting the European research from extra-EU interference.

2.2. *Key policy actions*

➞ « *Adopt a comprehensive and coherent approach at national as well as R&I sector level on safeguards while aiming for increasing levels of consistency across Europe at all levels*"

CNRS shares the need for a comprehensive and coherent approach, at both national and European levels. Because of national sovereignty issues, the organization and criteria for risk assessment will most likely vary from one Member State to another. At the EU scale, Research Security stakeholders should **build trust** amongst each

other, and **mutually accept each other's constraints and red lines**. Diverging appreciations of red lines between different partners of a European collaborative project should not be an obstacle to their participation to the project consortium.

➞ "*Invest in a better understanding of the sector-specific threat landscape and the sector's resilience*"

CNRS does share this need, yet being aware of all the challenges it poses. The threat landscape is in **continued evolution**. It can **greatly vary depending on the scientific topic or on the considered partners**; it is a matter of national sovereignty for each Member State.

➞ "*Support research performing organisations in their efforts to develop due diligence and risk management procedures and assign responsibilities within the organisation*"

Risk management and due diligence procedures are currently under review in institutions. The clear identification of players and responsibilities is a necessary step towards effective protection.

➞ "*Promote that national funding agencies incentivise beneficiaries to identify and address Research Security issues in their projects.*"

As a complement, **national and European funding agencies/programs should be identified as Research Security stakeholders**, and integrate this dimension in their operations. Funding decisions should take into account and facilitate Research Security.

2.3. *EU level initiatives*

➞ « *Facilitate peer learning and coordination among Member States and stakeholders and create communities of practice across Europe*"

As a French research performing organization, CNRS is willing to play an active role in these discussions and exchange practices with European communities. We propose that these communities be organized in groups of trust: the nature of the issues at stake in Research Security requires a certain level of trust among interlocutors. Besides, participants should commit to similar levels of engagement, to avoid one-way discussions.

➞ "*Support the development of practical guidance and due diligence tools for research performing organisations*"

The development of such tools would benefit all European stakeholders. Due diligence tools adapted to the research ecosystem are still lacking. In order to guarantee sovereign decisions in line with EU shared values, these tools should be **European tools**. The use of tools proposed by non-EU parties may put EU decision making at risk.

These tools should be made available to the entire European Research Security community. On the other hand, access to them should be limited to those players who need them for their decision-making. In particular, open accessibility (e.g. publication on the Internet) would expose which items are under vigilance, thus making it easier for malicious entities to try and bypass protective measures.

➞ "*Monitor the Member States' uptake of the Recommendation's guiding principles and key policy actions.*"

The application of these recommendations and their monitoring must respect the liability of institutions towards their national systems.

3. Additional comments

- States are accountable for the international treaties they have committed to, e.g. the Nuclear Non-Proliferation Treaty, or international conventions banning chemical and biological weapons, the Wassenaar Arrangement, the Missile Technology Control Regime, the Nagoya Treaty, etc. The European Research Security initiative must enable Member States to conform to their commitments.

- The general principles should include the notion of independence and resilience of the EU Research Security system with respect to possible actions of non-European third-party states. Caution should be taken to avoid the misuse of the EU Research Security initiative by non-EU parties to influence the European research protection.

- The "economic security" dimension must not be overlooked in the EU Research Security initiative; protecting EU assets is essential.

- According to our experience of PPST implementation, Research Security actors involve a broad spectrum of professional profiles: lawyers, scientists, international relations officers, former military personnel, IT experts, etc. This diversity of skills brought together in networks is definitely an asset. **The European Research Security initiative should build from such a diversity of skills**, preventing possible overfocus on certain aspects to the detriment of others (e.g.: legal compliance, cybersecurity issues, etc.). At the same time, the European Research Security initiative should include the setting up of specific training courses, so that - in all their diversity - those involved in Research Security share a common basis of skills.

- The EU Research initiative should provide support for training and awareness-raising for all research staff. In order to incorporate Research Security into research culture as early as possible, **young researchers may be particularly aimed at**.

- Research Security measures should be accompanied by secure, effective and consistent information security management.

- According to the Call for evidence statement, the level of awareness of the Research Security issue can vary greatly from one EU country to another. This situation may lead to pressures to exclude partners of countries that have little or no risk control measures from European consortia. Our practical experience of such situations shows actually the opposite: it occurs that a partner having a more stringent Research Security system be under pressure from partners who do not have the same level of protection. Consortia operating rules must take into account the different ways in which partners assess Research Security issues.