SAND2023-13389O

Study on Global Experiences on Research Security to Inform Armenia's Reform

Tatevik Davtyan

November 2023

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

CONTENTS

Openness and Security are not Contradictory but Complementary and Mutually Reinforcing.[1]

EXECUTIVE SUMMARY

1. **The report aims to guide key stakeholders within Armenia's research system in establishing research security frameworks and practices.** Drawing insights from policies, strategies, and initiatives implemented worldwide, the report aims to raise awareness among policymakers, research funding agencies, institutions, and other stakeholders about harmful practices that threaten the global research ecosystem. These include unauthorized access and transfer of information and technology by foreign states and non-state actors that can harm a nation's economic, strategic, and international security. Establishing a comprehensive policy framework and implementing protective measures are essential to safeguard Armenia's research system and contribute to the broader global efforts to secure research endeavors.
2. **The report delves into research security standards, both on a global scale and within the context of Armenia. It offers policy recommendations while providing insights into Armenia's scientific and research landscape, legal framework, and research security practices.** The report presents strategies and actionable steps to fortify research security in Armenia, emphasizing the need for a delicate balance between academic freedom and other values of research integrity with security and open international collaboration. It underscores the importance of safeguarding students, faculty, research, and intellectual property while promoting international research collaborations and ensuring transparency. Acknowledging the distributed responsibilities for research integrity and security among various stakeholders, including government bodies, funding agencies, research institutions, universities, and academic associations, it advocates for an inclusive policy framework. Such a framework should encompass all stakeholders and focus on raising awareness, prevention, effective response, and robust recovery mechanisms.
3. **This report emphasizes the importance of scientific progress, which relies on scientific freedom and international collaboration. However, it also brings attention to new challenges and threats due to some governments and non-state actors using forceful tactics to exploit and manipulate the open research environment for their own gain.** Unauthorized information transfer and foreign interference in public research are now seen as significant risks to national and economic security in many countries. As bastions of knowledge and innovation, universities and research institutions are prime targets for cyber threats, intellectual property theft, or other unauthorized access and transfer of sensitive research information.
4. **Addressing these challenges necessitates a nuanced, tailored approach, with shared responsibility among governments, funding agencies, research institutions, universities, and academic associations. These stakeholders are actively implementing measures to enhance research security and integrity globally. Governments** enacted regulations to oversee sensitive information, requiring research institutions, universities, and researchers to disclose conflicts of interest and commitment. Additionally, governments provide guidelines, checklists, and policies to raise awareness of research security risks and implement measures to mitigate them. **Funding agencies** employ guidelines to address conflicts of interest and

[1] See Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, “G7 Best Practices for Secure & Open Research”, May 2023, [https://www.safeguarding-science.eu/knowledge-security/];

commitment for applicants, reviewers, and agency staff. Many have incorporated risk assessments into their application and review procedures. This involves applicants filling out risk assessment questionnaires and collaborating with agencies and host institutions to formulate mitigation plans for identified national and economic security risks. **Research institutions** assess risks and may restrict involvement in high-risk activities. Some have restricted participation in high-risk foreign government-sponsored activities. **Universities** are developing rules and guidelines to safeguard research security and preserve scientific integrity and freedom. Dedicated committees and training programs raise awareness among researchers and staff. **Academic associations** are working on consensus guidelines and organizing workshops to raise awareness and share experiences. Some associations also establish local committees for advisory support to research institutions and universities. **At the intergovernmental level,** the G7 countries have established a working group to fortify the security and integrity of the research ecosystem. They aim to develop a standard set of principles to protect research and innovation collaboration from potential risks. The European Commission released a toolkit in early 2022 to counter foreign interference in research, innovation, etc.

5. **Armenia's current research landscape lacks a government strategy or policy addressing research security. However, ongoing initiatives in the research system lay the foundation for potential improvements. Aligning with European Union standards and models presents an encouraging framework for Armenia's research security initiatives.** The government's acknowledgment of emerging information security threats in the National Security Strategy 2020 reflects its commitment to establishing legal and institutional cybersecurity frameworks. This development holds promise for standardized information security practices across public and private organizations. In addition, government-led reforms in research funding, integration of public research and higher education R&D, and the enhanced role of the National Academy of Science promise to elevate research quality and provide an environment conducive to implementing security protocols. While the current export control laws mandate exporters to establish an internal compliance program encompassing controlled goods, including intangible assets and information, research institutions mostly lack these programs.

6. **This report presents recommendations to strengthen research integrity and establish research security practices in Armenia that require action from various actors, building on current efforts:**

    - Prioritize awareness-raising efforts by allocating government resources to promote dialogue and information sharing on research security and integrity. Establish forums for engagement between the government and the research community to identify risks, understand needs, and formulate supportive policies. Activities should encompass disseminating reports, organizing seminars, workshops, and stakeholder meetings, and aligning integrity principles with security measures. Highlight specific research areas at risk.

    - Collaborate with funders, institutions, and researchers to accurately identify sensitive research areas prone to risks. Educate the research community on the potential risks associated with specific areas, particularly those linked to military, intelligence, dual-use applications, economic benefits, sensitive data, critical infrastructure, and national interests.

- Create a working group, led by the government and involving all stakeholders, to develop a strategic policy document or conceptual framework for establishing and implementing research security practices.
- Collaborate with the Armenian Ministry of Education, Science, Culture, and Sport to comprehensively evaluate the existing security practices of research and higher education institutions.
- Evaluate funding agency processes based on this report's insights. Establish disclosure and conflict of interest/commitment requirements for institutions and researchers and strengthen the agency's management capabilities.
- Collaborate with higher education and research institutions to develop an internal compliance program for export control. Conduct a pilot internal compliance program with Yerevan State University. Offer training and workshops on creating and implementing these programs. Suggest changes to relevant laws and regulations to ensure they are effectively enforced if needed. Provide comprehensive training and ensure that authorities are actively enforcing the laws.

7. **The report draws on valuable literature and resources, incorporating best practices in research security.** It has been enriched with insights and information from various authoritative sources carefully selected from readily accessible repositories, including the National Science Foundation's Office of the Chief of Research Security Strategy and Policy (U.S.) and Safeguarding-Science.eu (Germany, EU).[2] These sources represent a compilation of the most reliable and well-regarded materials available on research security. This comprehensive approach ensures that the report is based on a solid foundation of knowledge and expertise in the field.

[2] See [https://www.dni.gov/index.php/safeguarding-science/research-security];[https://www.safeguarding-science.eu/knowledge-security/].

DEFINITIONS[3]

Term	Definition
Conflicts of interest (COI) & conflicts of commitment (COC)	A conflict of interest is a set of circumstances that create a risk that a secondary interest will unduly influence professional judgment or actions regarding a primary interest. A conflict of commitment is a situation in which an individual accepts excessive workloads or conflicting duties from multiple employers.
Detrimental research practices	Detrimental research practices are actions that violate the traditional values of the research enterprise and that may be detrimental to the research process. Detrimental research practices include misrepresentation, breach of duty of care, and improperly dealing with misconduct allegations. Theft, deception, and coercion are detrimental research practices that are more directly of concern concerning research security.
Dual-use research of concern	Dual-use research of concern can (based on current understanding) be reasonably anticipated to generate knowledge or technology that has the potential to be exploited to purposely cause harm and threaten public health or national security, although the research itself is conducted for beneficial purposes.
Due diligence	Due diligence is an analysis of an organization done in preparation for a transaction with that organization. In international research collaboration, due diligence includes inquiry into a partner's past activities, the sector that it operates in, the commercial and ethical standing of its governing body, and the legal and regulatory environment of the partner.
Freedom of scientific research	Freedom of scientific research encompasses the right to freely define research questions, choose and develop theories, gather empirical material, devise and employ sound academic research methods, to question accepted wisdom and bring forward new ideas. It entails the right to share, disseminate, and publish research results openly, including through training and teaching. It is the freedom of researchers to express their opinions without being disadvantaged by the system in which they work or by governmental or institutional censorship and discrimination. It is also the freedom to associate with professional or representative academic bodies and associated scientific meetings.
Foreign interference vs foreign influence	Foreign interference is carried out by or on behalf of a foreign actor and is contrary to national sovereignty, values, and interests. It is coercive, covert, deceptive, or corrupting. This is in contrast to foreign influence, which is part of normal diplomatic relations and is normally conducted in an open and transparent manner. While it can be useful in some circumstances to distinguish between interference and influence, the line between these two is not always clear.
Knowledge security	Knowledge security means preventing the unauthorized transfer of knowledge and technology. It also includes preventing covert influence by state actors on higher education and research, which can impair the freedom of scientific research either directly or via self-censorship.
Open science	Open Science can be defined as efforts by researchers, governments, research funding agencies or the scientific community to make the primary outputs of publicly funded research results – publications and the research data – publicly accessible in a digital format with no or minimal restriction as a means for

[3] The Glossary is based on **OECD Science, Technology, and Industry Policy Papers**, "*Integrity and Security in the Global Research Ecosystem*" June 2022, No. 130, [https://doi.org/10.1787/1c416f43-en]; at 17-19.

Term	Definition
	accelerating research. Broader definitions emphasize a closer relationship between science and society as part of Open Science.
Reciprocity	Reciprocity is the practice of exchanging research materials, outputs, and knowledge in a manner that benefits all collaborating partners. It is necessary for effective cooperation because it helps to ensure that cooperation is mutually beneficial, even if there may be asymmetries in the capacity of research partners to reciprocate cooperation or exploit its benefits.
Research ecosystem	Research systems involve different actors, including research funders, different types of research institutions and universities and individual researchers. These actors are interdependent, operating together in a dynamic ecosystem. Policy frameworks and formal or informal rules, norms and standards are all critical aspects of the governance of research ecosystems, which operate at different scales from local to global. The global research ecosystem is characterized by interactions between actors in different countries that have different national interests.
Research integrity	Research integrity is an overarching term that refers to the ethos of research Integrity may be attributed to individual researchers, but also to institutions or the entire research ecosystem. In this project, “research integrity” refers specifically to certain values, norms, and principles that constitute good scientific practice (freedom of scientific research, openness, honesty, accountability, etc.) and regulate international research collaboration (reciprocity, equity, non-discrimination, etc.). These apply to individual researchers, research institutions, and science as a social system, and to every stage of the research process.
Research misconduct	Research misconduct can be narrowly defined as fabrication, falsification, or plagiarism (FFP) in proposing, performing, or reviewing research or in reporting research results. Fabrication is making up data or results and recording or reporting them. Falsification is manipulating research materials, equipment, or processes or changing or omitting data or results such that the research is not accurately represented in the research record. Plagiarism is appropriating another person’s ideas, processes, results, or words without giving appropriate credit.
Research security	In a globalized research ecosystem, ensuring research security means preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests.
Science diplomacy	Science diplomacy is broadly understood as a series of practices that stand at the intersection of science and diplomacy. Science diplomacy has been divided into three phenomena: science for diplomacy – the use of science to advance diplomatic objectives; diplomacy for science – the use of diplomatic action to further scientific and technological progress; and science in diplomacy – the direct involvement of science or scientific actors in diplomatic processes.

1. PROBLEM STATEMENT

8. **Scientific progress hinges on two fundamental principles: scientific freedom and international collaboration.** Scientific freedom empowers researchers to autonomously choose their research areas and interpret findings, free from political or profit-driven influence.[4] It fosters knowledge, health, prosperity, security, and environmental protection. Simultaneously, universities and research institutions thrive on open communication, shared knowledge, and collaborative endeavors, propelling scientific advancement. Scientific freedom expedites discoveries and fosters openness within research communities. It lays the groundwork for global initiatives tackling urgent challenges like climate change, pandemics, and socio-economic issues that demand collective global solutions.[5]

9. **Core values and integrity principles must underpin international collaboration, while academic freedom must be exercised responsibly and dedicated to conducting and applying science with integrity.**[6] Both researchers and institutions must engage in fair, innovative, open, and trustworthy scientific practices at both the domestic and international levels. This can be achieved by adhering to professional values, principles, and best practices that uphold research validity, social relevance, responsibility, and quality,[7] referred to as research integrity. Although research integrity does not have a universal definition, it encompasses important values such as academic freedom, transparency, honesty, accountability, and other vital values, norms, and principles that constitute good scientific practice and regulate international research collaboration.[8]

10. **The evolving dynamics of international collaboration and the shifting landscape of scientific production raise considerable national and economic security concerns.** Some individuals and foreign governments disregard research integrity principles and values, creating the danger of unauthorized access and sharing of research knowledge. Malicious actors may exploit academic partnerships, physically infiltrate research facilities, engage in espionage, or exploit cyber security weaknesses to obtain research information and data. Insiders or outsiders can carry out these activities, which may have far-reaching implications for research collaboration, funding processes, training, and peer review.[9] While these actors are typically motivated and supported by the interests of foreign states or non-state entities, their actions violate research integrity and security norms and values. Research security aims to safeguard research communities against foreign state or non-state interference with research that jeopardizes economic, strategic, national, and international security.[10] Some examples of detrimental practices are described below.

    - ***Theft or misuse of data, samples, or know-how:*** Imagine you are the president of a research institution and a researcher in your institution who worked in several medical research labs, stole

[4] See **Council of the European Union, Conclusions**, *"Principles and values for international cooperation in research and innovation"* (June 2022), [https://www.consilium.europa.eu/media/56956/st10125-en22.pdf].

[5] See *G7 Best Practices for Secure & Open Research*, *Id.* at 2.

[6] See **AAAS Statement on Scientific Freedom & Responsibility**; [https://www.aaas.org/programs/scientific-responsibility-human-rights-law/aaas-statement-scientific-freedom].

[7] See *G7 Best Practices for Secure & Open Research*, *Id.* at 2-3.

[8] See **OECD Science, Technology, and Industry Policy Papers**, "*Integrity and Security in the Global Research Ecosystem"* June 2022, No. 130, [https://doi.org/10.1787/1c416f43-en]; at 18.

[9] See **European Commission, Directorate-General for Research and Innovation**, "*Tackling R&I foreign interference – Staff working document*", Publications Office of the European Union, 2022, [https://data.europa.eu/doi/10.2777/513746].

[10] See **OECD Science, Technology, and Industry Policy Papers** *Id. at 3.*

trade secrets, and transferred them to a foreign country after receiving payments from a foreign government, or

- ***Deceptive practices - failure to disclose foreign funding and affiliations:*** You are the head of a national funding agency, and a researcher funded by your agency did not declare any information about foreign funding and affiliations in his funding proposal while required to do so under the proposal and award policies of the national funding agency, or
- ***Deceptive practices - employment with a foreign military university:*** You manage publicly-funded projects on swarm systems for agricultural applications in an engineering and information technology institution. It was revealed in the media that a professor under your supervision was working on those projects and was affiliated as a professor at a foreign military university. He had not declared his role with the foreign university to his home institution or
- ***Coercive practices – foreign interference with publication:*** You are the president of a university, and a professor at your university published a paper on a foreign country's response to COVID-19, predicting a dire situation. The foreign country's Consulate approached your university to request the paper be retracted, and a public apology be issued because the paper criticized and embarrassed the foreign government or
- ***Coercive practices – participation in foreign talent and recruitment programs:*** You are a professor of an institution and were approached by a foreign university to become an adjunct professor in your field of expertise. The foreign university offered to cover all travel costs and pay you to deliver lectures and participate in research projects for three months during a summer semester. If you accept the position, you may be obligated or under pressure to disclose confidential or commercial information as a condition of the agreement or during the work term at the foreign institution or
- ***Cybersecurity - remote access information and threat taxonomy:*** You are a Ph.D. student from an academic laboratory and have been invited to attend an overseas conference in your area of specialization. You were asked to present research you are conducting on new agri-business drone capabilities. During the event, a foreign actor captured the information for remote access, and a permanent access link to the university's system and your research was established. Within a month of returning, your research had been copied, and prototypes were developed, appearing on the open market. Foreign countries also adopted drone technology for use in military operations or
- ***Foreign actor-funded center – theft of information:*** You are the president of a university, and a foreign actor finances and supports the establishment and staffing of a language and cultural center at your institution, which enables the spreading of propaganda, disinformation, and information manipulation and facilitates espionage, or
- ***Coercion of technology transfer officer- theft or misuse of data, samples, or know-how:*** You are a technology transfer officer at a research institution. A foreign actor recruits you, and you are subsequently coerced or blackmailed into gaining access to and sharing confidential research and IP or
- ***State-sponsored phishing campaign:*** You are a professor or a student of a higher education institution, and a foreign state-sponsored hacker group runs a phishing campaign on students and staff of your institution to harvest their accounts and gain unauthorized access to publications, data, and code or
- ***Disinformation campaign on social media:*** You are a researcher in a research group, and a foreign actor runs a disinformation campaign on social media targeting a research group or researchers at a research institution and discrediting their research on specific topics.[11]

[11] These examples are based on deceptive practices outlined in **OECD Science, Technology, and Industry Policy Papers,** *Id.,* at 26-31, and **European Commission, Directorate-General for Research and Innovation**, "*Tackling R&I foreign interference – Staff working document*," Publications Office of the European Union, 2022, [https://data.europa.eu/doi/10.2777/513746], at 12-13.

11. **One of the challenges in discussing research integrity, research security, and associated concepts is that definitions differ across countries and communities.** Having shared definitions of key terminology is important to build a common understanding and avoid misinterpretation. The 'working definitions' used throughout this document are briefly summarized in the Definitions table at the beginning.

12. **Foreign Interference is carried out by, or on behalf of, a foreign actor and is contrary to national sovereignty, values, and interests.** It is coercive, covert, deceptive, or corrupt. This contrasts with foreign influence, which is part of normal diplomatic relations and is normally conducted openly and transparently.[12] It can be useful to distinguish between interference and influence, but the boundary between these two is often blurred.[13] Nevertheless, research institutions and government stakeholders should differentiate between foreign interference and influence as frequently as possible and establish their own definitions for the two, even if the distinction is not always clear-cut.

13. **Goals and Implications.** Foreign actors may pursue economic, strategic, geopolitical, or military objectives and have various intended outcomes. These may include retrieving sensitive or confidential information, accessing network, and computing infrastructure, managing physical assets, core services, research equipment and data, software, publications, personal information, and intellectual property rights. Foreign actors may also aim to influence decisions that can provide a strategic and competitive advantage, favor collaborations and projects, and influence the selection of students and staff. Furthermore, foreign actors may undermine human rights, democracy, freedom of speech, the rule of law, and academic values such as academic freedom, openness, transparency, accountability, ethics, integrity, trust, privacy, and intellectual property rights.[14]

14. **Targets and Valuable Positions.** Universities and research institutions are a primary target for foreign bad actors because they are hubs of knowledge, innovation, and critical research. These institutions house a wealth of intellectual property, cutting-edge research findings, and valuable technological advancements. Additionally, the interconnected nature of research ecosystems in a globalized world makes universities vulnerable to cyberattacks and other security breaches. Common targets of foreign malign actors include **students**, **researchers**, administrative **staff** (HR, ICT, legal, financial, policy, and project management staff), and **research support staff**, including library, IPR, technology transfer, and research management staff.

15. **Tactics and Techniques Employed.** Foreign interference can take on many legal or illegal and non-transparent forms, such as undue influence, interference, or misappropriation of research. Interference can involve states, militaries, non-state actors, and organized criminal groups stealing research outcomes, ideas, and intellectual property. Bad actors may use various means to interfere, including through infrastructure (both digital and physical), people, and funding. Some

[12] See **University Foreign Interference Taskforce (2021)**, *Guidelines to Counter Foreign Interference in the Australian University Sector,* [https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector].

[13] See University Foreign Interference Taskforce (2021), *Guidelines to Counter Foreign Interference in the Australian University Sector*,[https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector]; Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor that is coercive, covert, deceptive, or corrupting and is contrary to the sovereignty, values, and interests of the European Union", see **European Commission, Directorate-General for Research and Innovation**, *Id* at 12.

[14] See *Id.* at 16.

tactics involve political pressure that may involve high-level representatives of national authorities or politically linked organizations pressuring decision-makers with favors or repercussions. Financial support can create dependencies through investments in large-scale projects and joint ventures in the local or foreign country, donations, funding for research projects or initiatives, and loans. Exploiting people may involve coercing or recruiting individuals through social engineering, bribes, blackmail, intimidation, and/or selecting and placing allied individuals in strategic positions. Digital intrusions may also be used, including phishing, hacking, malware, and local unauthorized access to digital networks and databases. Information manipulation may involve disseminating false or misleading information that discredits local viewpoints or promotes foreign viewpoints online, through social media, and in lectures and events. This may involve manipulating discourse using inauthentic accounts, fake websites, fake personas, and information suppression.[15]

16. **Finding a single, all-encompassing solution to address foreign interference and unauthorized access to research data is not feasible**. This is because the nature and scale of these challenges can vary widely across different research contexts, institutions, and regions. What works effectively in one situation may not be as effective in another. Universities and research institutions should develop tailored strategies to address their unique circumstances and challenges. This customization allows them to consider their research areas, international collaborations, and the geopolitical landscape in which they operate. For example, an institution conducting sensitive national security research might require more stringent security measures than an institution focused on open-source software development. Notably, the responsibility for combating foreign interference does not rest solely on one entity. It is a shared responsibility among various stakeholders, including governments, research funding agencies, research institutions, universities, and academic associations. Each of these parties plays a crucial role in maintaining the integrity and security of research endeavors. By working collaboratively and aligning their efforts, these stakeholders can collectively enhance research integrity standards and implement robust security measures. This helps to safeguard the foundational principles of research, ensuring that it continues to advance knowledge and benefit society while mitigating risks associated with foreign interference and unauthorized access.

[15] See **European Commission, Directorate-General for Research and Innovation**, *Id.* at 16-17.

2. GLOBAL EXPERIENCES IN RESEARCH SECURITY

2.1. Concepts of Research Security and Research Integrity

17. **Research integrity refers to certain values, norms, and principles that constitute good scientific practice (freedom of scientific research, openness, honesty, accountability, etc.) and regulate international research collaboration (reciprocity, equity, non-discrimination, etc.).**[16] While different countries interpret research integrity differently[17], most agree on the importance of having a set of principles and guidelines for individual researchers and institutions to follow good research conduct. Efforts have also been made to ensure research integrity and good research conduct in international collaborations.[18] Research integrity is the foundation of all research, forming the base to collaborate in a fair, innovative, open, and trusted environment.[19] The Singapore Statement on Research Integrity was created in 2010 at the World Conference on Research Integrity, which representatives from 51 countries attended. This statement outlines four key principles: honesty, accountability, professional courtesy and fairness, and good stewardship.

18. **Research security refers to the actions taken to protect against, identify, or mitigate the risks to science and research inputs, processes, and outputs from unauthorized access, theft, or espionage. It protects the integrity and health of the national and international research system and national and economic interests** by securing intellectual property, knowledge, and know-how and preventing unwelcome state and non-state parties' unfair exploitation of these assets. The Centre for Security and Emerging Technologies (CSET) in the United States defines research security as "preventing foreign actors from acquiring scientific research through means that are illegal or contrary to prevailing norms, such as rewards, deception, coercion, and theft." Thus, securing research in a globalized research ecosystem

[16] See **OECD Science, Technology, and Industry Policy Papers**, *Id.* at 17.

[17] See, e.g., **The Norwegian National Research Ethics Committees (2016***), "Guidelines for Research Ethics in Science and Technology"*, [https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/60126_fek_guidelines_nent_digital.pdf]; **Universities UK (2019)**, *"The Concordat to Support Research Integrity*",[https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-08/Updated%20FINAL-the-concordat-to-support-research-integrity.pdf]; **National Institutes of Health**, "*What is research integrity"* [https://grants.nih.gov/policy/research_integrity/what-is.htm]; **PricewaterhouseCoopers Aarata LLC (2021),** "*Research Integrity Investigation and Analysis Repor*t" [https://www8.cao.go.jp/cstp/english/doc/report_en.pdf]; **All European Academies (2017),** *"The European Code of Conduct for Research Integrity"* [https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf];

[18] See **World Conference on Research Integrity (2013)**, "*Montreal Statement on Research Integrity in Cross-Boundary Research Collaborations, Montreal statement"* (World Conference on Research Integrity), and Kivimaa, P. (2022), "Transforming innovation policy in the context of global security", Environmental Innovation and Societal Transitions, Vol. 43, pp. 55-61 [https://www.sciencedirect.com/science/article/pii/S2210422422000302?via%3Dihub].

[18] The Singapore Statement on Research Integrity was created in 2010 at the World Conference on Research Integrity. This statement outlines four key principles: honesty, accountability, professional courtesy and fairness, and good stewardship. These principles are further translated into a comprehensive framework of 14 responsibilities, covering critical aspects such as addressing research misconduct (such as falsification, fabrication, and plagiarism), determining authorship, maintaining rigorous peer review, disclosing conflicts of interest, and upholding research ethics.

[19] The Singapore Statement on Research Integrity was created in 2010 at the World Conference on Research Integrity. This statement outlines four key principles: honesty, accountability, professional courtesy and fairness, and good stewardship. These principles are further translated into a comprehensive framework of 14 responsibilities, covering critical aspects such as addressing research misconduct (such as falsification, fabrication, and plagiarism), determining authorship, maintaining rigorous peer review, disclosing conflicts of interest, and upholding research ethics.

means preventing undue political influence over research, undesirable dual-use applications of research findings, conflicts of interest and commitment, and cyber-attacks.[20]

19. **Research security, particularly in preventing foreign-state or non-state interference, is closely intertwined with research integrity. It's important to recognize that measures taken to enhance research security play a crucial role in fortifying research integrity.** For instance, adherence to research integrity entails a commitment to transparency. This includes openly declaring all potential conflicts of interest and commitment (financial or otherwise) that could impact research outcomes. These disclosures are vital to building public trust in research and influence the selection, funding, review, and research projects. Disclosing conflict of interest and commitment is attributable to research security measures. Hence, these measures can be essential in supporting research integrity and assessing potential security risks. This also extends to actions that could lead to the mismanagement of conflicts of interest and commitment or the fabrication, falsification, plagiarism, or destruction of research data. Research integrity entails freedom from harassment or coercion in the research process and actively promoting equity, diversity, and inclusion.[21] Therefore, ensuring research security - preventing foreign state or non-state interference with research – will also strengthen research integrity. Despite their synergies, research integrity and security sometimes present conflicting priorities. For instance, striking the right balance between these considerations is paramount for any university or research institution. Many institutions already have dedicated offices or administrative measures for research integrity, but there may be a gap in resources or understanding regarding research security. Bridging this gap is essential for comprehensive research governance.

20. **Research integrity is the cornerstone of domestic and international research.** It upholds values and best practices that ensure research quality, bolster confidence, and safeguard its integrity. Simultaneously, it involves implementing security measures to shield research from activities or behaviors that might compromise its integrity. National and institutional frameworks for research integrity need to include research security considerations.[22]

21. **Governments should integrate research security considerations into national and institutional frameworks for research integrity. Mitigating unauthorized information transfer and foreign interference must include research integrity and scientific responsibility considerations.** Security and risk management should be integrated into institutional culture and processes as an essential aspect of research integrity. Countries can expand the remit of national research integrity offices, where these already exist, or may wish to establish a dedicated national contact point or center of expertise for research security within the government to work with counterparts across the research ecosystem.

[20] See **OECD Science, Technology, and Industry Policy Papers**, *Id.* at 65.

[21] See **Group of Seven G7 Working Group** on *the Security and Integrity of the Global Research Ecosystem (SIGRE)* (June 2021), at 5 [https://www.bmbf.de/SharedDocs/Downloads/de/2022/220812-g7-sigre-paper.pdf?__blob=publicationFile&v=2].

[22] See Figure 1: A graphic depicting how research security and research integrity protect the foundation of research in **Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group**, "*G7 Best Practices for Secure & Open Research", at 4.*

2.2. Common Values of Research Integrity & Principles of Research Security

22. **The common values of research integrity apply broadly to all research community members, including governments, research funders, research institutions, and individual researchers.** These values include academic freedom, institutional autonomy, and the ethical conduct of research, which entails respecting the rights of those who develop ideas, research outcomes, and intellectual property throughout the research project's lifecycle, including their publication rights.[23] In alignment with established research integrity principles, the G7 nations have established Common Values of Research Integrity (see **Table 1**) and Principles of Research Security (see **Table 2**). While acknowledging that different countries may interpret these values differently, the overarching objective remains consistent: collectively identifying and addressing research integrity and security concerns. Security and risk management should be integrated into institutional culture and processes as an essential aspect of research integrity.

23. ***Common Values of Research Integrity*** **highlights the fundamental importance of academic freedom, freedom from discrimination, equity, institutional autonomy, open science, public trust, and transparency in ensuring the security and integrity of research endeavors.** *Academic freedom* emphasizes the need for researchers to operate in an environment free from external influence. *Freedom from discrimination and harassment* underscores the necessity of a secure space for all researchers. *Equity and inclusion* contribute to a diverse and secure research community. *Institutional autonomy* protects research missions from undue external pressure, *open science* balances transparency with security, and maintaining *public trust* is vital. Lastly, *transparency and honesty* are essential for research integrity and security, promoting ethical conduct and collaboration in pursuing knowledge.

24. ***Principles of Research Security*** **emphasize the importance of a balanced scientific research and collaboration approach.** *Scientific merit and excellence* should guide funding decisions, but consideration of national and economic security risks is also necessary where relevant. *Open science* is encouraged, but there should be limits to ensure safeguards are in place, especially when research could have ethical, geopolitical, or security implications. *Collaboration and dialogue* are crucial, with governments sharing information to address common risks. *Proactive efforts, risk proportionality, shared responsibilities*, and *accountability* are emphasized to manage and reduce research security and integrity risks effectively. Additionally, *adaptability* is key to avoiding rigid approaches that may hinder beneficial research and fail to address emerging risks.

[23] See **OECD Science, Technology, and Industry Policy Papers**, *Id.* at 11.

Table 2. Common Values of Research Integrity[24]

Term	Definition
Academic Freedom	The freedom to teach, conduct, and publish research in an academic environment that emphasizes enabling all participation is a fundamental tenet of research. It is fundamental to the mandate of research institutions to pursue truth, provide education to students, and disseminate knowledge and understanding. Academic freedom requires an environment of enabled autonomy and job security where researchers are free from undue external influence or limitations on scholarly inquiry.
Freedom from Discrimination, Harassment, and Coercion	Freedom from discrimination, harassment, and coercion is a value that is foundational to the success of research. All research community members should be free from discrimination, harassment, bullying, coercion, or threats to their personal or family safety. Discrimination, harassment, and coercion can be by an individual, a group, an institution, or a government. This includes instances whereby entities may coerce and harass individuals to act in unethical and dishonest ways – counter to their will or interest – to support an entity's objectives, interests, and directives.
Equity, Diversity, and Inclusion	Equity, diversity, and inclusion (EDI) is the active promotion of the principles of access, diversity, and non-discrimination in all research activities – including recruitment procedures and career prospects. These are necessary for all aspects of research. EDI contributes to the diversity of identity and thought, with room for various ideas, cultures, and views. Ensuring everyone can freely participate in the research community, ecosystem, or enterprise will help build an innovative, prosperous, and inclusive world.
Institutional Autonomy	Research institutions can only fulfill their missions to students, faculty, staff, and society if they pursue and disseminate knowledge based on evidence, data, and peer review. Institutions should be free to pursue their missions. These missions can be based on the oversight and direction of their governance or can be to meet community and local needs. Regardless, institutional autonomy requires a safe and secure environment in which all individuals and institutions are free and protected from unwanted external influence.
Open Science and Access to Research	All members of the research community should actively support the open sharing and exchange of research results, data, methods, and inputs while preserving the incentives for innovation. Open science –making science and research inputs, outputs, and processes available to all with minimal restrictions – should be practiced in full respect to privacy, security, and ethical considerations, as well as appropriate protection of ideas, research outcomes, and intellectual property. Enabling all members of society to build on previously validated research, open science helps to speed up the pace of discoveries, bettering the lives of others and our societies and contributes to research quality.

[24] See **Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group**, "*G7 Best Practices for Secure & Open Research",* Annex A, at 13-14.

Term	Definition
Fostering Public Trust	Conducting and pursuing research to maintain the trust of the public and all those involved in research is vital to the continued success of science and research efforts. As contributors to integrity, all entities engaged in science and research activities should strive to demonstrate that they can meet the expectations of trust when accessing sensitive data or research. This requires deliberate, clear, and shared understanding across all partners of the research results' purpose, use, and ownership. This understanding should be upheld and respected across all stages of the research and in all jurisdictions.
Transparency, Disclosure, and Honesty	Fully transparent and reciprocal sharing of the methods, data, and outcomes of unclassified research – while maintaining confidentiality when appropriate – is crucial to research collaboration, integrity, and the free flow of ideas and information. Transparency in disclosing researcher affiliations, competing or conflicting interests, and funding sources is also important to ensure the research's integrity. Transparency requires honesty. As a complementary value, honesty entails being straightforward and free of fraud and deception when proposing, developing, undertaking, reviewing, reporting, and communicating research. This extends to all aspects of research and includes the acknowledgment of the work of others and making justifiable claims or sensible interpretations based on research findings.

Table 2. Principles on Research Security[25]

Term	Definition
Balancing National and Global Interests	Funding for scientific and research partnerships should continue to be guided primarily by scientific merit assessments and excellence and take appropriate and proportionate consideration and mitigation of risks to national and/or economic security where necessary.
Maintaining Openness and Research Security	Open science should not be an afterthought, and governments should commit to making research accessible when there is no justification for it to remain closed. It is recognized that openness should have limits and not override obligations to maintain safeguards over research that could have adverse ethical, geopolitical, or national security implications should it be disseminated.
Collaboration and Dialogue	All entities involved in research should strive to support and engage with one another in pursuing a community that upholds security alongside openness. Governments should commit to engaging in meaningful information sharing about the nature of the risks to address common risks alongside researchers and benefit from shared approaches.

[25] See *Id.*, Annex B, at 15

Term	Definition
Proactive Efforts	Governments should strive to take proactive and preventative measures to manage and reduce research security and integrity risks based on lessons learned and best practices.
Risk Proportionality	Responses to risks should be proportionate and appropriately scaled. Risk-appropriate responses to research security should consider the potential for misuse of the research and the aggregate level of risk, among other factors.
Shared Responsibilities	To address dynamic and changing research risks, all research community members should acknowledge and understand their distinct roles and responsibilities with respect to addressing and managing risks to research security and research integrity.
Accountability and Responsibility	Individuals and organizations should be held accountable for all their actions, including when their behaviors deviate from accepted standards.
Adaptability	There should be a commitment to dynamic research security measures, acknowledging that overly rigid approaches risk delaying beneficial research. Static and unwavering approaches can lead to significant research disincentives and do not account for new and emerging risks.[26]

[26] See **Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group**, "*G7 Best Practices for Secure & Open Research",* May 2023; [https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/2023_bestpracticepaper.pdf]

2.3. Balancing International Collaboration, Research Integrity, and Security

25. **Open international collaboration catalyzes the exchange of ideas, data, and expertise, propelling advancements in various fields. However, this openness is not without its perils, including increasing an institution's vulnerability to intellectual property theft, unauthorized access to sensitive data, and the potential misuse of research for unethical ends.** Openness can challenge core integrity values such as academic freedom and institutional autonomy, as described below. While export control systems primarily target sensitive technologies for national security and non-proliferation objectives, regulating the intangible transfer of data, especially in fundamental research, proves complex. Fundamental research often enjoys exemptions from export controls; however, many areas considered fundamental research may hold dual-use potential, like artificial intelligence and quantum computing. This potential can spark economic rivalries among nations, corporations, and regions. Traditional laws have effectively safeguarded intellectual property rights, but protecting data, information, and know-how in the internet age presents new complexities. Restricting access to such information may also counter research integrity principles and the spirit of open science.[27]

26. **Academic freedom stands as the cornerstone of academic pursuits, encompassing the freedom of academic staff and students to engage in research, teaching, and communication without external interference or fear of reprisals.** It grants researchers the liberty to define research questions, develop theories, collect empirical data, and employ research methodologies to challenge existing paradigms and introduce novel ideas. Academic freedom extends to disseminating research results through publication and teaching, free from censorship imposed by institutions or governments.[28] It shields researchers from any adverse consequences from expressing their opinions within the academic realm. Freedom in academic inquiry and university autonomy are universally recognized as crucial components of a thriving research system. Simultaneously, international collaboration, equity, and non-discrimination constitute vital facets of a well-functioning global research ecosystem. The challenge lies in striking a balance between fostering open and trust-based international scientific collaboration and enacting protective, albeit potentially constraining, regulations for research security.[29]

27. **Academic freedom encounters challenges in the research security context as universities and research institutions navigate a complex geopolitical landscape where research outcomes hold significant national interests.** Consequently, home governments may shield research outcomes from foreign interference, placing the onus on universities to implement measures to mitigate security-related research risks. This may lead to imposing new rules and regulations that influence academic freedom.

28. **Countries undergoing autocratization or established autocracies may exert repressive controls that extend beyond their borders.** Such controls manifest through various means, including monitoring citizens working abroad, demanding regular reporting to embassies, encouraging scholars and students to surveil one another, digitally monitoring communications (including virtual classrooms), detaining critical scholars upon their return to their home countries, and even targeting their families. Repressive controls may also involve pressuring publishers to censor content and inserting restrictive clauses into cooperation agreements,

[27] See **OECD Science, Technology, and Industry Policy Papers**, *Id.* at 24.

[28] The EU recognizes the "essential freedom for scientific research" as a universal right protected by global agreements and EU treaties. The Bonn Declaration, supported by EU Member States, reaffirms this commitment. The Bologna Process also emphasizes academic independence, integrity, and student-staff involvement.

[29] See [https://stip.oecd.org/stip/research-security-portal].

effectively making them accomplices in violations of academic freedom. Covert efforts such as funding, honorary titles, paid positions, and privileges can be employed to co-opt scholars and institutions, posing a threat to academic freedom and integrity. Normalizing political control over academic institutions and fostering agreements with research institutions in repressive contexts erodes academic integrity, creates an environment of fear, and hinders scholars from pursuing truth, all stemming from conflicts of interest and divergent principles. Importantly, activities detrimental to academic freedom can originate from actors within autocratic countries as well as those in democratic settings, where for-profit research funders may prioritize their interests over robust research, universities might engage in self-censorship through agreements, and academic publishers may heed censorship directives from foreign governments or other entities.[30]

29. **Balancing open international collaboration, research integrity, and security is challenging.** The collaboration should be as open as possible and as closed as necessary. Over-regulation or excessive intervention can affect the freedom of scientific inquiry and exchange. In contrast, the lack of shared and respected international regulations and norms can lead not only to the misappropriation of research but also to certain types of research being selectively conducted in countries that do not impose legal or ethical restraints. Policies are needed to facilitate common global approaches that promote trusted international collaboration and the open exchange of ideas without government interference.[31] The measures to reduce the risk of foreign interference should be proportionate and not endanger the scientific process, which relies on collaboration and knowledge sharing.

2.4. Research Security Policies and Initiatives: Countries at the Forefront

30. **This section explores the actions taken by various stakeholders in research security in countries such as the United States, the United Kingdom, Canada, Australia, Japan, Germany, and the Netherlands.** Various measures implemented by main stakeholders are as follows: (a) **National governments** have established regulations and guidance that encompass disclosure requirements, research security programs, risk assessment, mitigation, and information sharing between main stakeholders; (b) **Funding agencies** have instituted policies for research funding participants, recipients, proposal reviewers, and agency staff. These policies are designed to manage conflicts of interest and commitment effectively; (c) **Public research institutions** have implemented various measures to address security and integrity concerns in research collaborations, including risk assessment tools, guidelines for international collaboration, and approval processes for external funding; (d) **University associations** have created guidelines, tools, and best practices to help universities assess and mitigate security-related risks in research collaborations, fostering responsible and secure internationalization; (e) **Universities** have implemented policies, oversight structures, and training programs to address research security, conflicts of interest, and research integrity concerns, promoting responsible research practices and safeguarding against security risks.

31. **Several multinational initiatives have been undertaken to safeguard the research and innovation ecosystem against potential risks to open and reciprocal research collaboration. The G7 countries** have established the Security and Integrity of the Research Ecosystem (SIGRE) working group to develop common principles. This group plans to create a

[30] See **European Commission, Directorate-General for Research and Innovation**, "*Tackling R&I foreign interference – Staff working document," Id.*, at 25-26.

[31] See **OECD Science, Technology, and Industry Policy Papers**, *Id.* at 24-25.

virtual academy and toolkit to encourage collaboration among researchers, innovators, business leaders, and policymakers, fostering a deeper understanding of research integrity and security. **The European Commission** has published a toolkit outlining best practices for mitigating foreign interference in research and innovation. **The Asia-Pacific Economic Cooperation (APEC)** forum has established guiding principles for research integrity, emphasizing transparency and disclosing conflicts of interest. **Science Europe and the Global Research Council** have initiated discussions on research ethics, integrity, and culture, leading to the development of principles and practices addressing research security, particularly in the context of rapidly evolving research. **The Global Science Foundation and the OECD-GSF Secretariat** appointed an international Expert Group to develop a report that presents an overview of the ongoing discussion regarding integrity and security within the global research ecosystem. It outlines seven comprehensive recommendations, including actionable suggestions, involving coordinated efforts from multiple stakeholders.

2.4.1. United States of America

32. **Disclosure Legislation and Presidential Memorandum.** The U.S. Congress passed legislation requiring disclosure of funding sources in federal research and development awards applications.[32] The U.S. Government has also issued a presidential memorandum (NSPM -33) to improve cooperation between law enforcement and funding agencies and strengthen government-supported research protection.[33] This is accompanied by implementation guidance, which addresses disclosure policy (ensuring that federally-funded researchers provide their funding agencies and research organizations with appropriate information concerning external involvements that may bear on potential conflicts of interest and commitment), oversight and enforcement (ensuring that federal agencies have clear and appropriate policies concerning consequences for violations of disclosure requirements and interagency sharing of information about such violations); standardized disclosure requirements across agencies and digital reporting tools that facilitate easy compliance; and, ensuring that research organizations that receive substantial federal R&D funding maintain appropriate research security programs.[34]

33. **Cooperation, Awareness, and Engagement.** More effective cooperation and exchange of information between intelligence agencies, law enforcement agencies, research institutions, and universities is considered necessary. The NSPM-33 requires the Director of the Office of Science and Technology Policy (OSTP) to work with the Director of National Intelligence (DNI) and other agency heads to increase awareness of potential risks to research security and integrity and policies and measures for addressing those risks. Therefore, the U.S. Government

[32] See 116th Congress (2021), *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, [https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf]; [https://context-cdn.washingtonpost.com/notes/prod/default/documents/aee24ba6-7289-4d79-8c68-f62c6c02e808/note/4b0d58fa-277f-4177-814b-4ac323b20f54.].

[33] See The White House (2021), *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/?utm_source=link.

[34] See The White House (2021), *Clear rules for research security and researcher responsibility*, [https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security- and-researcher-responsibility/] National Science and Technology Council (2022), *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-supported Research and Development*, https://www.whitehouse.gov/wp- content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

suggests that institutions establish relationships with local Federal Bureau of Investigation (FBI) offices to enhance both parties' communication and understanding of concerns.

34. **Regulations and Guidelines on Conflicts of Interest.** The United States Government has released guidelines to enhance the security and integrity of the nation's science and technology research enterprise.[35] These guidelines recommend that research organizations establish policies about conflicts of interest (COI) and conflicts of commitment (COC), standardize disclosure requirements, provide researchers with training on responsible research practices, and impose adequate consequences for non-compliance with disclosure requirements. Requirements on declarations of COI or COC are targeted at funding applicants, researchers working on projects supported by a funding agency, peer reviewers, and research agency staff.[36] In addition to regulations and guidelines, the U.S. Government Accountability Office (GAO) recommends that funding agencies have written procedures to address cases of failure to disclose required information, such as foreign affiliations. The written procedures outline investigation processes, including roles and responsibilities, and include administrative or enforcement actions that may be taken if allegations are substantiated. The administrative or enforcement actions available to a funding agency include asking the researcher's university to open an investigation, suspending grants, or referring cases for prosecution.[37]

35. **NSF Prohibitions, Research Security Chief, and DOE's Science and Technology Risk Matrix.** The U.S. National Science Foundation (NSF) forbids its staff from participating in foreign government talent recruitment programs. It has created the Chief of Research Security Strategy and Policy, responsible for developing and implementing strategies to improve research security and the agency's coordination with other federal agencies.[38] The U.S. Department of Energy (DOE) prohibits its employees and contractors from working in the DOE complex while concurrently participating in certain foreign government-sponsored talent recruitment programs or foreign government-sponsored or affiliated activities. The DOE has developed a Science and Technology Risk Matrix to identify areas of critical emerging research that do not have regulatory control mechanisms but may warrant additional protective measures due to their national or economic security implications.[39]

36. **Academic Associations and Core Values.** The Association of Public Land-grant Universities (APLU) and the Association of American Universities (AAU) in the United States recently

[35] See National Science & Technology Council (2021), *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*, [https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf]

[36] It includes disclosure on professional preparation (e.g., educational degrees), organizational affiliations, academic, professional or institutional appointments, and current and pending support of all R&D projects regardless of whether the support is a direct monetary contribution or in-kind contribution current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs, visiting scholars funded by an external entity, students and postdoctoral researchers funded by an external entity, paid consulting that falls outside of an individual's appointment; separate from institution's agreement, travel supported/paid by an external entity to perform research activities with an associated time commitment, certification by the individual that the information disclosed is accurate, current, and complete.

[37] See Government Accountability Office (2020), *Agencies Need to Enhance Policies to Address Foreign Influence*, [https://www.gao.gov/assets/gao-21-130.pdf].

[38] See National Science Foundation (2020), *NSF creates new research security chief position*, [https://www.nsf.gov/news/news_summ.jsp?cntn_id=300086].

[39] See United States Department of Energy (2021), *Unclassified Foreign National Access Program*, [https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b]

published The University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus.[40] The report outlines how universities can ensure research security, protect against intellectual property theft and academic espionage, and prevent undue foreign government influence or infringement on core academic values. The AAU and the APLU also suggest maintaining fundamental principles and values such as academic freedom, free expression, inclusion, diversity, transparency, collaboration, and the declaration of possible conflicts of interest and respect for intellectual property to address security concerns. They also call on the government to reduce administrative barriers to establishing collaborations and agreements with international researchers, both informal and formal.[41]

37. **University Policies and Oversight.** The University of Texas at Austin developed a policy under which researchers must complete a Financial Interest Disclosure and mandatory training.[42] Similar policies have been developed by the University of Michigan and Rochester University. Rochester University's interim guidelines cover all aspects of research collaboration, whether on campus or abroad, and require disclosure of international collaboration and support, such as talent programs, grants, and gifts. Many other U.S. universities have also adopted this requirement. Additionally, Rochester University monitors visitors, including students, faculty, researchers, and short-term visitors like lab and facility visitors, guest lecturers, and speakers, to ensure compliance with their policies. The University of Michigan has a Research COI Committee responsible for reviewing the outside activities of researchers whose research proposals will be sponsored.[43] This committee aims to determine if any external activities could significantly impact the research design, conduct, or reporting. By doing so, the committee ensures that researchers' interests do not unduly influence their primary obligations to science, sponsors, the university, colleagues, or students. If any conflicts of interest are identified, the committee develops strategies to manage them properly. The University also provides research ethics and compliance training through the Program for Education and Evaluation in Responsible Research and Scholarship. This program offers online training modules covering research integrity, conflicts of interest, export controls, and research information security. While the training was initially only required for those working on federally funded projects, all faculty, staff, and students involved in scholarship and research are now expected to complete it.

38. **Role of Academic Associations.** The National Academies of Sciences, Engineering, and Medicine in the United States has launched a National Science, Technology, and Security Roundtable.[44] The roundtable brings together individuals from research agencies, national

[40] See Association Public Land-grant Universities (APLU); Association of American Universities (AAU); (2020), *University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus*, https://www.aplu.org/members/councils/governmental- affairs/CGA-library/effective-science-and-security-practices---what-campuses-are-doing/file.

[41] See Association of American Universities (AAU) and Association of Public Land-grand Universities (APLU) (2021), *Principles and Values to Guide Actions Relevant to Foreign Government Interference in University Research*, https://www.aau.edu/key-issues/principles-and-values- guide-actions-relevant-foreign-government-interference-university.

[42] See The University of Texas at Austin (n.d.), *Conflict of interest, conflict of commitment, & outside activities*, [https://provost.utexas.edu/policies-and-compliance/conflict-of-interest].

[43] See University of Michigan (n.d.), *Conflict of Interest (COI)*, [https://research- compliance.umich.edu/conflict-interest-coi]

[44] See National Academies of Sciences, Engineering and Medicine (2020), *Co-chairs appointed to lead new national science, technology, and security roundtable*, https://www.nationalacademies.org/news/2020/10/co-chairs-appointed-to-lead-new-national- science-technology-and-security- roundtable#:~:text=Roundtable%20%7C%20National%20Academies-,Co%2DChairs%20Appointed%20to%20Lead%20New,Science%2C%20Technology%2C%2 0and%.

intelligence, law enforcement, academic research, and business communities. It identifies and considers security risks involving federally funded research and development, identifies effective approaches for communicating risks to the academic and scientific community, and shares best practices for mitigating them.

39. **JASON's Toolkit for Principal Investigators.** A group of independent scientists from the U.S., known as JASON, has put forward a set of questions that principal investigators must consider before collaborating with foreign research organizations. American researchers have been using these questions as a tool or checklist.[45]

2.4.2. United Kingdom

40. **UK Government's Intervention in Asset Acquisitions.** The UK government can intervene in certain acquisitions, especially those involving assets in 17 sensitive areas of the economy, under the National Security and Investment Act. This includes assets owned by universities or public research institutions that are being sold. The responsibility to inform the government of such transactions lies with the seller.[46]

41. **Compliance for International Students Pursuing Sensitive Subjects.** International students who wish to pursue postgraduate studies in certain sensitive subjects in the UK must comply with the Academic Technology Approval Scheme (ATAS) before starting their studies. This scheme, established by the Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office, requires students from specific countries to obtain an ATAS certificate to study these fields in the UK.[47]

42. **Promoting Integrity in International Research Collaboration.** Guidelines and checklists promote integrity in international research collaboration, particularly in critical areas like STEM subjects, emerging technologies, and commercially sensitive research. These guidelines were developed in consultation with the research and university community and include a checklist for researchers to assess their research proposals. Additionally, guidance on export controls applied to academic research has been published.[48]

43. **Research Collaboration Advice Team (RCAT).** RCAT advises researchers to protect their work from hostile activities and ensure secure international collaboration. Their guidance covers

[45] JASON (2019), *Fundamental Research Security*, https://nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[46] See Department for Business, Energy & Industrial Strategy (2021), National security and Investment Act: guidance for the higher education and research-intensive sectors, https://www.gov.uk/government/publications/national-security-and-investment-act-guidance- for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act- guidance-for-the-higher-education-and-research-intensive-sectors].

[47] See Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office (2013), *Academic Technology Approval Scheme (ATAS)*, https://www.gov.uk/guidance/academic- technology-approval-scheme.

[48] See The UK's Centre for the Protection of National Infrastructure (CPNI) Centre for the Protection of National Infrastructure (CPNI) (n.d.), *Trusted Research Guidance for Academics*, https://www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Academi a.pdf. has published Trusted Research Guidance for Academia. (see Box 6.1) (Centre for the Protection of National Infrastructure (CPNI), 2020. In addition to the Trusted Research Guidance for Academia, the UK Export Control Joint Unit (2021) Centre for the Protection of National Infrastructure (CPNI) (2020), *Trusted Research Guidance for Academia*, https://www.cpni.gov.uk/trusted-research-guidance-academia. Centre for the Protection of National Infrastructure (CPNI), *Checklist: Evaluating research proposals*, https://www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academi a.pdf. Government of the United Kingdom (2021), *Export controls applying to academic research*, https://www.gov.uk/guidance/export-controls-applying-to-academic-research

export controls, cyber security, and intellectual property protection. RCAT serves as a single point of contact in the government, responding to universities identifying potential risks in ongoing projects or proposals. They also proactively engage with research institutions to provide support and guidance.[49]

44. **The Centre for the Protection of National Infrastructure (CPNI) Workshops and STEM Universities Forum.** CPNI collaborates with academic partners in the UK to organize workshops aimed at helping universities manage national security risks associated with research. These workshops are designed to assist scholars in identifying and addressing security risks in international research collaborations. In 2021, the CPNI STEM Universities Forum was established to facilitate the confidential sharing of information related to secure research collaboration. Forum members include STEM research-intensive universities, organizations, CPNI, and the National Cyber Security Centre. Government and arms-length bodies may also be invited to participate when relevant.

45. **UK Research and Innovation (UKRI) Expectations and Due Diligence.** UKRI has established clear expectations for the research it supports, outlining funding policies, terms, and conditions. These expectations are supported by guidance and an active funding assurance or audit program. UKRI has also published principles that outline its expectations for organizations it funds regarding due diligence in international collaboration.[50] In addition, the guidance outlines declaration of interest requirements, where funding applicants are supposed to declare the following: personal remuneration from organizations or project partners involved in the proposed research (other than the named employing organization), significant shareholdings, or other financial interests in organizations that are involved in or might benefit from the research, research support (financial or in-kind) from commercial organizations involved in the grant or might benefit from the outcome of the research that is not mentioned in the application, un-remunerated involvement with any organization named on the application or which might benefit from the research or its outcomes, political/pressure group associations, and/or relevant known interests of family members and persons living in the same household.[51]

46. **Risk Assessment in Grant Applications.** Several UK research councils and the Wellcome Trust include a question on grant application forms that require applicants to assess the potential risks of misuse of their proposal. Guidance on risks of misuse is provided to external experts who peer-review grant applications. If serious concerns about the risk of misuse cannot be resolved through agreed-upon management strategies with host institutions, the application may not be funded. Researchers are expected to notify funders and host institutions of any new risks related to dual-use research that emerge during a project.[52]

47. **Universities UK (UUK) Guidelines for Managing Internationalization Risks.** UUK, the representative organization for UK universities, has published guidelines to help universities

[49] See Government of the United Kingdom (2021), *Dedicated government team to protect researchers' work from hostile activity*, https://www.gov.uk/government/news/dedicated-government-team- to-protect-researchers-work-from-hostile-activity

[50] See UK Research and Innovation (2021), *UK Research and Innovation Trusted Research and Innovation Principles*, https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821- TrustedResearchandInnovationPrinciples.pdf.

[51] UK Research and Innovation (UKRI) (n.d.), *Declaration of Interests: Applicants*, https://www.ukri.org/wp-content/uploads/2020/11/UKRI-261120-Declaration-of-Interests-for- applicants-v2.pdf.

[52] See Medical Research Council (MRC), Biotechnology and Biological Sciences Research Council (BBSRC), and Wellcome Trust (2021), *Managing Risks of Research Misuse: joint policy statement*, https://www.ukri.org/publications/managing-risks-of-research-misuse-joint-policy-statement/.

protect themselves, staff, and students while managing internationalization risks.[53] The guidelines offer key actions and case studies for university governing bodies and leaders, emphasizing the importance of awareness, understanding, and institutional resilience in mitigating international security threats. UUK affirms that senior university leaders can improve institutional resilience to security-related issues by developing a risk-aware culture. UUK also recommends that universities consider reputational, ethical, security, and financial risks. Actions include knowing partner institutions, making risk-informed decisions, establishing robust agreements, and defining clear roles and responsibilities for staff. Due diligence processes are essential for assessing security-related risks and protecting staff and students working abroad.

48. **The UK's Royal Society** provided input on the Foreign Influence Registration Scheme (FIRS) as the UK government considered it.[54] The Society acknowledged the potential dangers posed by hostile activities such as theft, misuse, or exploitation of research and the risk of compromised personal information. Failure to address these threats could harm the reputations of individuals and institutions and sometimes even pose a broader threat to society. However, the Society also highlighted the risk that overly strict regulations could discourage academic research and deter international collaboration. This feedback has helped establish the important factors to consider and balance in developing effective policy action.

2.4.3. Canada

49. **National Security Guidelines for Research Partnerships.** Researchers involved in international partnerships, especially those handling sensitive data, must assess potential national security risks associated with their work. The National Security Guidelines for Research Partnerships[55] outline sensitive research areas requiring special consideration, particularly those with dual-use potential or subject to controlled goods regulations. These guidelines aim to prevent foreign interference, espionage, and unwanted knowledge transfer that could benefit states or groups posing a threat to Canada or that may enable the disruption of the Canadian economy, society, and critical infrastructure. The guidelines identify sensitive research areas and apply them to federal research partnership funding, but all researchers are encouraged to use them to assess and mitigate risks. Researchers must complete a risk assessment form when submitting federal research partnership funding program applications.

50. **Policy Statement on Research Security and COVID-19.** The Policy Statement[56] encourages members of the research ecosystem in Canada to be aware of potential risks to their work during the COVID-19 pandemic. It emphasizes protecting knowledge creation and innovations while supporting Open Science and global research response efforts.

[53] See Universities UK (2020), *Managing Risks in Internationalisation: Security Related Issues*, https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing- risks-in-internationalisation.pdf.

[54] See Royal Society (2021), *Royal Society Submission to Home Office Consultation on Legislation to Counter State Threats*, https://royalsociety.org/topics-policy/publications/2021/royal-society- submission-to-home-office-consultation-on-legislation-to-counter-state-threats/.

[55] See Government of Canada (2021), *Executive summary of national security guidelines for research partnerships*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98256.html

[56] See Government of Canada (2020), *Policy statement on research security and covid-19*, https://www.canada.ca/en/innovation-science-economic-development/news/2020/09/policy- statement-on-research-security-and-covid-19.html.

51. **Online Training Courses for Researchers.**[57] The Canadian government has developed self-paced online courses, including "Introduction to Research Security" and "Cyber Security for Researchers," to train researchers and university staff. These courses are designed to raise awareness of key security information and can be accessed through the Safeguarding Your Research portal.

52. **The Government of Canada - Universities Working Group.**[58] The government has established the Government of Canada-Universities Working Group, which brings together universities, government departments, federal granting councils, and national security agencies. This working group was created to promote open and collaborative research while safeguarding research activities and maximizing the benefits for Canadians.

53. **Conflict of Interest and Confidentiality in Research (Government of Canada).** This document outlines guidelines for managing conflicts of interest and confidentiality in research within the Canadian government. Funding applicants and peer reviewers must declare professional or personal benefits resulting from the funding opportunity or application being reviewed, a professional or personal relationship with an applicant or the applicant's institution, and/or a direct or indirect financial interest in a funding opportunity or application being reviewed.[59]

54. **Risk Assessment for NSERC Alliance Grants Program.** The Natural Science and Engineering Research Council's (NSERC) Alliance Grants Program has introduced a risk assessment process for grant applications. When applicants identify risks related to their research, they are required to develop risk mitigation plans. The funding agency reviews these risk assessment questionnaires and mitigation plans and may refer them to national security agencies or relevant government departments when risks are identified. This process ensures that research funding decisions consider potential national security concerns.

55. **Mitigating Economic or Geopolitical Risks in Sensitive Research Projects.** The U15 Group of Canadian Research Universities[60] has published a guide that provides practical advice and best practices for assessing and mitigating economic and geopolitical risks in sensitive research projects. The guide includes checklists and matrices to assess risks related to project teams, non-academic partners, cybersecurity, data management, research findings, and international travel.

56. **Research Partnership Security Checklist for International Partnerships.**[61] The University of Toronto has developed a Research Partnership Security Checklist to assist principal investigators in evaluating the suitability and potential risks of engaging with international partners before starting specific projects.

[57] See Government of Canada (2021), *Safeguarding your research*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html

[58] See Government of Canada (n.d.), *About us*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98090.html

[59] See Government of Canada (2016), *Conflict of interest and confidentiality*, http://www.science.gc.ca/eic/site/063.nsf/eng/h_90108244.html?OpenDocument

[60] See U15 Group of Canadian Research Universities (2019), *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects*, https://telfer.uottawa.ca/assets/research/documents/docs/Mitigating-economic-and-or- geopolitical-risks-in-sensitive-research-projects-dec-2019.pdf.

[61] See University of Toronto (2021), *Research Partnership Security Checklist for International Partnerships*, https://www.utsc.utoronto.ca/research/sites/utsc.utoronto.ca.research/files/docs/Research- Partnership-Security-Checklist-for-International-Partnerships.pdf.

2.4.4. Japan

57. **Monitoring Sensitive Technology Transfer.** Technology transfers through domestic transactions in Japan have not been deemed as exports. Still, the national government has begun to control sensitive technology transfers between domestic residents whom foreign governments or companies might influence. Residents who receive significant financial benefits or have contracts (such as employment contracts) from foreign governments or companies will be considered as potentially influenced by foreign governments or companies.

58. **Japanese Government's Policy Directions for Research Integrity.** Japan's national government has established policy directions to ensure research integrity in response to new risks associated with research internationalization and openness.[62] Researchers must report information on foreign financial support and affiliations to their research institutions and funding agencies. Revised guidelines on public research funding in 2021 facilitated the storage of required information in the Cross-ministerial R&D Management System (e-Rad)[63] to reduce administrative burdens on researchers. Failure to report information may result in bans on future research funding applications for up to five years. The national government conducts seminars to educate research institutions, universities, and researchers on the new policy directions and provides template checklists to facilitate compliance.

2.4.5. Australia

59. **University Foreign Interference Taskforce (UFIT).** Australia established the UFIT, which created guidelines to counter foreign interference in the Australian university sector.[64] UFIT collaborates with universities and government agencies to address foreign interference risks. UFIT guidelines cover governance, due diligence, communication, risk, and cybersecurity education. The guidelines are complemented by guidance material that includes case studies, tool kits, and best-practice guides. These guidelines were refreshed in 2021 to address evolving foreign interference threats and assist universities in better identifying and responding to risks.[65]

60. **Australian Research Council's Conflict of Interest and Confidentiality Policy**. All parties involved in the funding process, including applicants, peer reviewers, and funding agency staff, must disclose their professional positions, committee memberships in other organizations, consultancies, and any foreign financial support (cash or in-kind) received for research-related

[62] See Integrated Innovation Strategy Promotion Council (2021), *Regarding the Response Policy for Securing Research Integrity Against New Risks Associated with the Internationalization and Openness of Research Activities*, https://www8.cao.go.jp/cstp/tougosenryaku/9kai/siryo1- 2.pdf.

[63] See [https://www.e-rad.go.jp/en/]. e-Rad is run by nine ministries and agencies in charge of open research funding systems and is developed and operated by the Cabinet Office with cooperation from other ministries and agencies. The Cross-Ministerial Research and Development Management System (e-Rad) is a cross-ministerial system enabling online management of research and development work through the Competitive Research Funding System run by Japanese ministries and agencies and other open research funding systems. In addition to supporting processes from acceptance of applications to results reports, the system prevents unwarranted duplication and overconcentration of researchers' research and development costs.

[64] The Australian Minister for Education. The University Foreign Interference Taskforce is a joint initiative of the Australian Department of Education, Skills, and Employment and the Department of Home Affairs.

[65] University Foreign Interference Taskforce (2021), *Guidelines to Counter Foreign Interference in the Australian University Sector*, https://www.dese.gov.au/guidelines-counter-foreign- interference-australian-university-sector/resources/guidelines-counter-foreign-interference- australian-university-sector. The Taskforce's Guidelines to Counter Foreign Interference in the Australian University Sector were developed jointly through a steering group and four working groups (Research and Intellectual Property, Foreign Collaboration, Cyber Security, Communication and Culture) with approximately 40 members from universities and government agencies, including intelligence agencies.

activities. They must also disclose any current or past affiliations with foreign-sponsored talent programs within the last decade and any associations with foreign governments, political parties, state-owned enterprises, and military or police organizations. Additionally, they must disclose any involvement in boards of directors, advisory groups, professional relationships, family and personal relationships, and financial interests, including any compensation received in the form of cash, services, or equipment from other parties supporting research activities.[66]

61. **Research Engagements Sensitivities Tool (REST) by CSIRO**. In 2020-2021, Australia's Commonwealth Scientific and Industrial Research Organization (CSIRO) developed the REST to assess foreign interference risks when considering new research opportunities systematically. The final decision maker's rank for project approval corresponds to the assessed risk level of the project. High-risk projects require approval from the CEO. CSIRO shares its tools and expertise in risk assessment with Australian universities.

2.4.6. Germany

62. **German Research Foundation (DFG) and Leopoldina Guidelines.**[67] DFG and the National Academy of Sciences Leopoldina have created guidelines to reduce the risk of misuse in research and promote self-regulation among individual researchers, research institutions, and universities. The guidelines suggest that individual researchers should conduct risk analyses, minimize risks, responsibly publish sensitive results, and avoid research that poses a high risk of misuse. Research institutions and universities should develop ethical rules for handling security-related research and comply with legal regulations. Furthermore, the DFG requires that research project applications include handling security-related aspects. Applicants must evaluate whether their proposed projects involve immediate dual-use risks, and if they do, present a risk-benefit analysis and describe measures to minimize them. If research institutions or universities have research ethics committees, the committees must be consulted beforehand, and their statements must be included in the research proposals.[68]

63. **Max Planck Society and Leibniz Association Guidelines.**[69] The guidelines recommend researchers identify and minimize risks relating to human rights, academic freedom, and scientific espionage before they start international collaboration. In addition, administrative headquarters need to approve third-party funds before researchers can accept such funds.[70] When researchers have questions about rules, an ombudsperson can provide them with confidential advice.[71] Like the Max Planck Society, the Leibniz Association requires its

[66] See Australian Research Council (2020), *ARC Conflict of Interest and Confidentiality Policy*, https://www.arc.gov.au/policies-strategies/policy/arc-conflict-interest-and-confidentiality- policy/arc-conflict-interest-and-confidentiality-policy.

[67] See German Research Foundation (DFG) and German National Academy of Sciences Leopoldina (2014), *Scientific Freedom and Scientific Responsibility*, https://www.dfg.de/download/pdf/dfg_im_profil/geschaeftsstelle/publikationen/stellungnahmen_papiere/2014/dfg-leopoldina_forschungsrisiken_de_en.pdf.

[68] See German Research Foundation (DFG) (n.d.), *Proposal Preparation Instructions*, https://www.dfg.de/formulare/54_01/54_01_en.pdf.

[69] See Max Planck Society (2021), *Guidelines for the Development of International Collaborations of the Max-Planck-Gesellschaft*, https://www.mpg.de/16784189/mpg-guidelines-for-international- cooperations-2021.pdf.

[70] See Max Planck Society (2021), *Guidelines for Responsible Conduct*, https://www.mpg.de/18156413/leitplancken.pdf.

[71] See Max Planck Society, *Ombudspersons*, https://www.mpg.de/about- us/organisation/ombudspersons

institutions and researchers to assess political situations in partner countries and the associated motivation of research partners.[72]

64. **German Rectors' Conference Guidelines**[73] provide rules or international partnerships for German universities. The guidelines are based on the principles of freedom of research, the added value of joint research, scientific, ethical, and legal standards observance, equal partnership, and promoting researcher mobility. Ethical and legal standards include laws for protecting intellectual property and regulations on handling security-related research.

65. **German Academic Exchange Service Support.** The German Academic Exchange Service offers guidelines and assistance to help universities assess international partnerships.

66. **German Academy of Sciences Leopoldina** regularly organizes conferences and workshops on handling security-relevant research and invites experts from various disciplines.[74] The events aim to raise awareness among researchers of security-relevant aspects of their research and to share experiences. Participants discuss specific security-relevant research projects and whether self-regulated restrictions for researchers can prevent dystopian malicious use scenarios. The German Academy of Sciences Leopoldina helps German research institutions and universities establish local committees responsible for ethics in security-relevant research. Currently, 130 local committees or contact persons are actively helping the research community in ethical assessments of security-relevant research projects.[75] [76]

67. **Guidelines for Avoiding Conflicts of Interest.**[77] The guidelines outline circumstances for disclosing conflicts of interest among peer reviewers. **Automatic exclusion includes certain circumstances resulting in the exclusion of** close personal relationships, financial interests in the proposal's success, ongoing or planned scientific collaborations, conflicts related to university roles, extended employment or supervisory relationships, affiliation or transfer conflicts. **Individual Case Evaluation** includes circumstances handled on a case-by-case basis, such as other personal ties or conflicts, financial interests of specific individuals, additional affiliation or transfer concerns, participation in various university bodies, recent research collaborations, involvement in appointment processes, and recent mutual review processes.

[72] See Leibniz Association (2021), *Risk Management in International Scientific Cooperation – points to consider*, https://www.leibniz- gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/%C3%9Cber_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf.

[73] See German Rectors' Conference (2020), *Guidelines and Standards in International University Cooperation*, https://www.hrk.de/resolutions- publications/resolutions/beschluss/detail/guidelines-and-standards-in-international-university- cooperation/.

[74] See German National Academy of Sciences Leopoldina (n.d.), *Conferences and workshops of the Joint Committee on the Handling of Security-Relevant Research*, https://www.leopoldina.org/en/about-us/cooperations/joint-committee-on-dual-use/dual-use- conferences-and-workshops/.

[75] See German National Academy of Sciences Leopoldina and German Research Foundation (DFG) (2020), *Joint Committee of the DFG and Leopoldina on the Handling of Security-Relevant Research - Third Progress Report*, https://www.leopoldina.org/uploads/tx_leopublication/2020_Progress_Report_Joint_Committe e_Dual_Use.pdf.

[76] See German National Academy of Science Leopoldina (n.d.), *Contact persons and commissions in Germany responsible for ethics of security-relevant research*, https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use/kommissionsliste/?tx_leoinstitutions_institutionslist%5Baction%5D=list&tx_leoinstitutions_institutionslist%5Bcontroller%5D=List&cHash=8e12faffd7dcfa05a6ef95703d72a04a

[77] See German Research Foundation (DFG) (n.d.), *Guidelines for Avoiding Conflicts of Interest*, https://www.dfg.de/formulare/10_201/10_201_en.pdf.

2.4.7. Other Countries

68. **Country-Specific vs. Country-Agnostic Policies.** Some national policies identify specific countries as "sensitive" for research collaboration due to potential foreign interference, while others maintain country-agnostic policies. Country-specific policies help institutions focus on risk management but may risk prejudice and discrimination, while country-agnostic policies recognize that sensitive partnerships can emerge from unexpected sources.

69. **Netherlands' Knowledge Security Measures.**[78] The Netherlands is creating guidelines, checklists, and self-evaluation tools for research institutions and universities to ensure knowledge security when collaborating internationally. Knowledge security refers to preventing unauthorized transfers of knowledge and technology and covert influencing by state actors that may lead to self-censorship and hinder academic freedom. The government plans to establish a knowledge security center as a go-to resource for research institutions and universities seeking assistance with decision-making and responding to inquiries.

70. **Netherlands' Knowledge Security Advisory Teams.**[79] A Knowledge Security Advisory Team exists in every university. This virtual Team comprises relevant experts on safety risk management, information security, and international collaboration, and it can co-opt additional experts on specific research topics, countries' human resource issues, etc. This team supports the executive board of a university to make decisions on knowledge security issues. When a small university does not have all the expertise needed to assess knowledge security risks, the university can 'borrow' expertise from a Knowledge Security Advisory Team at another university.

71. **Contractual Requirements in Norway and Portugal.** In Norway, projects funded by the National Research Council are governed by contracts requiring compliance with laws, regulations, ethical guidelines, and research standards. Portugal's administrative law mandates conflict of interest (COI) declarations for those involved in the grant review process.

72. **Ethics and Integrity in Research in Norway**. The Act on Ethics and Integrity in Research requires all research institutions and universities to provide education in research ethics, including misuse of new technologies, to all employees and researchers.[80] As these initiatives already explicitly address issues related to research integrity and misuse of new technologies, it is easy to imagine that they can be extended, as necessary, to address broader issues relating to research security. Likewise, there are undoubtedly many other education and training activities in universities worldwide that could be readily adapted to incorporate research security.

[78] See Ministry of Education, Culture and Science (2020), *Knowledge Security in Higher Education and Research*, https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in- higher-education-and-research. Association of Universities in the Netherlands (VSNU) (2021), *Framework Knowledge Security Dutch Universities*, https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Integrale%20veiligheid /VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf.

[79] See Association of Universities in the Netherlands (VSNU) (2021), *Framework Knowledge Security Dutch Universities*, https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Integrale%20veiligheid /VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf.

[80] See Langtvedt, N. (2020), *The act on ethics and integrity in research*, https://www.forskningsetikk.no/en/resources/the-research-ethics-library/legal-statutes-and- guidelines/the-act-on-ethics-and-integrity-in-research/

73. **Swedish Foundation for International Cooperation (STINT) Guidelines.**[81] STINT has developed Responsible Internationalization guidelines with key questions to address potential risks limiting academic freedom in international collaboration.

74. **Research Ethics Education at Lund University.** In Sweden, Lund University requires all PhD students to take a research ethics course. The course aims to provide a foundation of research integrity and knowledge of research ethics, including ethical challenges in developing and implementing new technologies.[82]

[81] See Shih, T., A. Gaunt and S. Östlund (2020), *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration*, https://www.stint.se/wp- content/uploads/2020/02/STINT Responsible_Internationalisation.pdf.

[82] See Lund University (2020), *Research Ethics*, https://www.student.lth.se/fileadmin/lth/genombrottet/Course_Plan Research_Ethics_2021__GEM090F__ENG_.pdf.

3. ARMENIA'S RESEARCH SECURITY LANDSCAPE

3.1. General Observations on Armenia's Research System

1. **Due to its role in the industrial and research and development (R&D) system of the former Soviet Union, an independent Armenia inherited a diverse and developed network of research institutes, notably those under the National Academy of Science (NAS), and higher education institutions (HEIs) focused largely on education with limited research activities.** After Armenia's independence in 1991, the prevailing structure in Armenia's research and higher education system, which remains partly in place today, reflects a clear division. Research activities are primarily conducted by research institutes (RIs) of NAS or those funded by and reporting to specific ministries, so-called branch RIs. Meanwhile, HEIs primarily focus on teaching, with limited involvement in research. However, some universities have recently begun to engage in research activities. The NAS offers master's and Ph.D. programs through its International Scientific-Educational Centre, established in 1997.[83] Although research is no longer exclusively confined to NAS institutions, Armenia's research system remains fragmented, with over 69 research-performing organizations, including 13 universities.

2. **The Armenian Government (AG) aims to address the fragmentation of the R&D system and tackle other challenges, including governance and research funding. The government has developed a new *Draft Law on Higher Education and Science*[84] to replace the current *Law on Higher and Post-Graduate Education.*[85]** The government focuses on consolidating the public and higher education R&D sector and implementing other reforms based, among others, on fundamental problems identified in certain field evaluation reports.[86] These problems concern the strategy and operation of the Armenian science system, including the governance of the science system (strategic and operational authority), the vision and role of the science system in future national development, the funding system for science, and the institutions and structure of the research-performing system.[87]

3. **To improve the research sector, the AG seems to follow recommendations[88] urging to establish a national evaluation process that will assess all research institutions every five years to help prioritize government funding, link research funding to performance to ensure it is effective (this means that direct appropriations will be combined with performance-based research funding) and bridge the gap between**

[83] It was established in 1997. See [https://www.sci.am/about.php?langid=2].

[84] See [https://www.e-draft.am/projects/4788/about].

[85] See [https://pdf.arlis.am/178451].

[86] In October 2018, the Ministry of Education, Science, Culture and Sport (MESCS) of Armenia confirmed a request to the European Commission (Directorate General for Research and Innovation) for the Horizon 2020 Policy Support Facility (PSF) to assist in reforming and reinforcing the performance of Armenia's research institutions and enhancing cooperation between higher education and research institutions. See Specific Support to Armenia Raising the bar: a new mission for science in Armenia's development. February 2020; DOI:10.2777/84398 [https://www.researchgate.net/publication/340384879_Specific_Support_to_Armenia_Raising_the_bar_a_new_mission_for_science_in_Armenia's_development].

[87] Background Report Specific Support to Armenia. Horizon 2020 Policy Support Facility. Prepared by the independent expert Sevak Hovhannisyan [https://ec.europa.eu/research-and-innovation/sites/default/files/rio/report/Background_report_Armenia.pdf].

[88] See supra note 4 and 5.

the research and higher education systems. The recommendations also suggest **consolidating higher education institutions** into a limited number (five or six) of full universities that conduct both higher education and research to enhance the quality of research-based education; **providing for stricter accreditation and licensing** processes for higher education institutions by setting a minimum number of students per course and establishing capital requirements for them; **enhancing research-oriented teaching staff** by requiring university teaching staff to conduct research and giving researchers from research institutions full access to teaching positions at higher education institutions; **transforming the role of NAS** into a learned society, with NAS research institutions becoming legally independent entities focused on scientific information, advisory services, and science diplomacy; **increasing the share of expenditure on R&D** as a percentage of GDP by 2025; **expanding and funding doctoral education initiatives**, with eventual scaling up to fully develop doctoral studies in Armenia; and **establishing inter-institutional centers of excellence** and competence based on updated research and innovation priorities.

4. **There are three potential scenarios to be considered by the government reforming research and higher education systems to enhance research-based education and scientific research.** These scenarios include: (i) maintaining the current status quo with three main types of RIs, encouraging collaboration and voluntary mergers between RIs on a case-by-case basis; (ii) integrating the NAS and other RIs into higher education institutes, with the staff of RIs becoming personnel of the universities (however, Armenian universities may lack the capacity to provide a suitable framework for RIs to conduct quality research), and (iii) strengthen university-based research and restructure NAS and other RIs into one or more publicly supported research organizations[89] (in this approach, researchers may have dual status as personnel at universities and institutes, and public RIs may be co-located at universities).[90]

5. **Armenia's HEIs are categorized into four types - universities, institutes, academies, and conservatories - offering various academic and research programs. There are over 60 recognized institutions, including 22 state universities, 37 private universities, four intergovernmental agreement-based universities, and nine foreign university branches.** However, some unaccredited private institutions may no longer be operational, reducing the number of functioning private universities to around 10. This abundance of universities is partly attributed to a weak vocational education system, leading to a broad coverage of topics in higher education. University (Hamalsaran) provides undergraduate and postgraduate education in various fields as well as carries out scientific research; Institute (Institut) conducts specialized and postgraduate academic programs and scientific research in one or more scientific, economic, or cultural branches; Academy (Akademia) conducts programs preparing and re-training highly qualified specialists as well as post-graduate programs; and Conservatory (Konservatoria) provides graduate and post-graduate programs in music.

6. Armenia's public research institutions are categorized into three groups: NAS RIs, consisting of research institutes under the National Academy of Science; Branch RIs, encompassing sector-specific research institutes funded by and reporting to specific ministries or government agencies; and HEIs RIs, including research institutes within Higher Education Institutions, such as university labs and institutes.

[89] E.g., CNRS in France, Fraunhofer, Leibniz, Helmholtz, and Max-Planck institutes in Germany, etc.
[90] See supra note 4 and 5.

7. **The scientific community in Armenia is facing considerable challenges. The system is strained due to insufficient funding and an aging scientific workforce, exacerbated by emigration and unfavorable career conditions such as low salaries and limited access to equipment and funding. RIs have decreased from 124 to 83, and the number of scientists has reduced from 25,344 in 1991 to 5,000-6,000 over the last thirty years,**[91] mostly due to Armenia transitioning towards a mixed economy model, while it previously served a large command economy and military-industrial complex. Despite these difficulties, Armenia's research output, measured by publications per million population, surpasses other Eastern Partnership countries. Additionally, the proportion of cited publications in the total output is higher than in Lithuania and Ireland and slightly below that of Estonia and Israel.[92] Most of Armenia's scientific output is in the natural sciences, accounting for 71.6% of publications in 2018, with physics and astronomy exhibiting a particularly strong presence (indicated by an H-Index of 146). The National Academy of Science remains the most successful research performer. NAS comprises 35 research institutes and centers specializing in five main disciplines, including mathematical and technical sciences, physics and astrophysics, natural sciences, chemistry, and earth sciences, and Armenology and social sciences. Through the Ministry of Education, Science, Culture and Sport, the state oversees 47 institutes, while the remaining are private. **Another feature of the Armenian research system is its relatively high rate of international co-publication.** This is partially attributed to longstanding collaboration in physics and astronomy and strong international connections with the Armenian diaspora in Western Europe and North America. Consequently, Armenia's scientific community still possesses the potential to excel on the international scientific stage in specific areas.

[91] See supra note 4 and 5.

[92] See supra note 4 and 5.

3.2. International R&D Cooperation and Mobility

8. Armenia is party to several cooperative R&D partnerships that are international in scope. Since 1992, Armenia has collaborated with the Joint Institute for Nuclear Research (JINR), which focuses on theoretical and experimental studies in particle physics, nuclear physics, and the physics of concentrated environments. As a member of JINR, Armenia established a coordinating committee led by the chairman of the State Committee of Science. Armenia joined the International Scientific and Technical Centre (ISTC) on 14 September 1994. Thus far, almost 400 projects involving 75 research institutes have been funded by ISTC, with a total of USD 36.5 million provided to 154 projects. Joint collaborative programs and the creation of joint labs and research centers are preconditions for networking toward EU programs. Furthermore, the Science Committee of Armenia has bilateral programs with several countries worldwide. **Table 3 includes bilateral programs that Armenia is a party to.**[93]

Table 3. Bilateral Programs Armenia is Party To

Program	Duration	Partner Country
Centre National de la Recherche Scientifique (CNRS) France	From 2009: 2 Joint Labs, 1 Joint Group, 20 Ann. Grants	France
Foundation for Fundamental Research (FFR)	From 2011: 30-34 Two Years Grants	Belarus
Russian Foundation for Humanities (RFH)	From 2011: 10-12 Two Years Grants	Russia
Russian Foundation for Basic Research (RFBR)	From 2013: 40-42 Two Years Grants	Russia
Federal Ministry of Education and Research (BMBF)	From 2013: 10 Two Years Grants	Russia
State Science and Technology Committee (SSTC)	From 2015: 4 Two Years Grants	Belarus
National Science Fund (BNSF)	From 2020	Bulgaria
National Research Council (CNR)	From 2020	Italy

[93] See supra note 5, at 23-24 - source: Science Committee of the Republic of Armenia.

9. **Armenia places significant importance on collaborating with the EU for R&D**. This is prioritized in national policy documents, such as the Strategy of STI Development for 2011-20 and the Action Plan for 2017-20. The goal is to support the development of Armenia's knowledge-based economy and be competitive in the European Research Area (ERA) through smart specialization. One of the main programs is the EU4 Innovation in Armenia project (2017-2020) to enhance STEM fields in Armenia that focus on investing in human capital that meets the demands of the local labor market. The project's estimated cost is EUR 26,125,000, with the EU contributing EUR 23,000,000. Another main program driving Armenia's research sector is Horizon 2020, which provides funding for research projects. From 2014-2016, Armenian researchers submitted 91 applications for funding, of which 12 were approved. Since May 2016, Armenia has been an Associated Country with the EU's Horizon 2020 program, giving Armenian researchers and innovators full access to the funding program. To date, 25 joint projects have been implemented, which align with Armenia's science and technology development priorities. **Table 4 shows Armenia's participation in the Horizon 2020 projects.**

Table 4. Armenia's Participation in Horizon 2020 Projects

Legal Name	H2020 Participation
National Academy of Sciences of the Republic of Armenia	7
Institute for Informatics and Automation Problems of the National Academy of Sciences of the Republic of Armenia	4
Small and Medium Entrepreneurship Development National Centre of Armenia Fund	3
Information Society Technologies Centre	2
Yerevan State University	2
Yerevan State Medical University after Mkhitar Heratsi	1
Centre for Ecological-Noosphere Studies National Academy of Sciences of the Republic of Armenia	1
Caucasus Consulting Group-am	1
ACBA leasing credit organization closed joint stock company	1
Grovf LLC 1	1
Educational and Cultural Bridges	1
Centre of Medical Genetics and Primary Health Care	1
'Matenadaran' M.Mashtots Institute of Ancient Manuscripts	1
Scientific and Production Centre Armbiotechnology NAS Republic of Armenia	1
Institute for Physical Research of the National Academy of Sciences of Armenia	1
A.I. Alikhanyan National Science Laboratory	1

10. **Armenia is included among the associated countries that participate in Horizon Europe; the new version of the Horizon 2020 program that is active until 2027. Under Horizon Europe, associate countries that engage in research partnerships with the EU are required to adhere to certain standards, such as disclosing conflicts of interest and upholding academic freedom as a right.** These standards closely align with the objectives of research security that are discussed in this paper. It is worth mentioning Horizon Europe as an opportunity for Armenian institutions to secure funding and collaborate with the EU, and implementing research security policies can help position Armenian research institutions more favorably in this regard.[94]

11. **Armenia engages in research cooperation with other countries in the region**. Armenia's **Centre for Ecological-Noosphere Research** has hosted UNESCO's 'Education for Sustainable Development Chair since 2011 through the UNITWIN/UNESCO Chairs Program. Armenia was active in the **Black Sea Interconnection (BSI)** project, which was executed as part of the European Union's Seventh Framework Program (FP7). The BSI project was initiated in March 2008 and was the largest research network project in the region. It aimed to improve the internet capabilities of research networks significantly. The project was modeled on NATO's Virtual Silk Highway and aimed to establish a robust research and education network in the South Caucasus region by connecting it to GÉANT2. The project aimed to integrate the scientific potential of the South Caucasus with Europe and foster collaboration among like-minded scientific communities. Over the past five years, the Institute for Physical Research of NAS has actively participated in more than 40 international grant programs, including FP7, ISTC, INTAS, CRDF, NFSAT, Volkswagen, ANSEF, and SCOPES. They partner with France, Germany, USA, Italy, UK, Russia, Latvia, Bulgaria, Poland, Japan, Spain, Australia, Switzerland, Croatia, Canada, Taiwan, Greece and other countries. The CNRS LIA (French-Armenian International Associated Laboratory) focuses on physics, chemistry, mathematics, humanities, and social sciences. The project was launched on January 20, 2009.

12. A**rmenia and Russia maintain a strong cooperation in research activities.** In March 2005, the Science Committee of Armenia and the Russian Foundation for Fundamental Research entered a collaboration agreement. Additionally, there are joint laboratories between the two countries, including the 'X-rays optics' laboratory between the Institute of Applied Problems of Physics and Tomsk Polytechnic University, the laboratory between the Institute of Applied Problems of Physics and Kurchatov Institute in Moscow, and the 'Optics of photons and elemental particles' international laboratory between the Republic of Armenia and Belgorod State National Research University. In March 2018, the Science Committee of Armenia and the Russian Foundation for Fundamental Research discussed a program promoting collaboration among young researchers and scientists. The Russian-Armenian University also plays a significant role in this partnership, signing agreements with top Russian universities like Moscow State University, Peoples' Friendship University of Russia, and Moscow State Institute of International Relations.

[94] See [Horizon Europe (europa.eu)]

3.3. Key Players in Research Governance

13. **The Ministry of Education, Science, Culture and Sport of Armenia (MESCS) is the executive authority of the Republic of Armenia, which elaborates and implements educational, science, culture, and sports policies.** On May 8, 2019, by the law of the Republic of Armenia "On Amendments and Addenda to the Law on Structure and Activities of the Government," the Ministry of Culture, the Ministry of Sport and Youth Affairs, and the Ministry of Education and Science were merged into the Ministry of Education, Science, Culture and Sport of the Republic of Armenia.

14. **The Higher Education and Science Committee (HESC)** [95]**:** A state body functioning within the MESCS. It manages the science budget, plays an active role in strategic planning and policy development in the field of science and education, preserves and develops the scientific and technical potential of the country, support the integration of science, education, and industry, supports international scientific/academic cooperation/integration, including integration in the European Higher Education Area and European Research Area, supports the development of economically viable competitive high technology (including dual-use) products, fosters the commercialization of scientific and technological outputs and their integration into the economy, ensures the regular operation and development of the science sector, promotes academic freedom and autonomy of higher education and research institutions.[96]

15. **The National Academy of Science (NAS) was founded by the Republic of Armenia as the highest self-governing scientific organization with a special status, which organizes, performs, and coordinates fundamental and applied research required for knowledge-based economic, social, and cultural development. It is directly subordinate to the Government.** The NAS proposes a list of top-priority fundamental and applied scientific research directions; ensures creating favorable conditions for developing scientific schools, training highly qualified scientific workers, and enhancing the skills of scientists and specialists; and implements other functions prescribed by the law. The Academy's main funding comes from a specific State budget line, but it can also participate in competitive calls organized by the SC for additional funding and projects. NAS was founded in 1943 and is based in Yerevan, with branches in Gyumri, Sevan, Goris, Vanadzor, and Ghapan. It employs over 3800 people, including approximately 340 Doctors of Sciences and about 1100 candidates of sciences. It has 33 academicians, 45 corresponding members, 5 Honorary members, 116 Foreign members, and 43 Honorary doctors, all elected at the General Meeting held once every three years. The Academy consists of a Presidium and 35 affiliated research institutions, with the Presidium having five divisions supervising the research institutions. The General Meeting of the Academy, which includes Full Members (academicians), Corresponding Members of the Academy, and authorized representatives of the scientific organizations of the Academy, is the Governing Body of NAS. The Presidium, composed of 15 members, administers the Academy between General Meetings.[97]

16. **Until recently, the Armenian science governance system lacked consultative bodies for research and innovation policy advice to the Parliament or the Government. The NAS's Presidium fulfills the advisory role of science to the government, but being a**

[95] See [http://hesc.am/en/e05fcf734e3a707251301869].

[96] See [http://hesc.am/files/statute-eng.pdf].

[97] See [https://www.sci.am/about.php?langid=2].

major beneficiary of state science funding means the NAS cannot be a neutral observer. Additionally, there are limited structured mechanisms for research and innovation stakeholders, such as education, business, and civil society, to provide input on formulating research and innovation policy and funding priorities. By the Prime Minister's Decision N1195-A of November 30, 2023, the Science and Technology Development Council of Armenia, led by the Prime Minister, was created[98]. The council was established to focus on science, technology, engineering, and mathematics (STEM) education, the development of applied science and technology, and the enhancement of the effectiveness of state programs implemented in these areas.

17. **Various organizations play distinct roles in promoting business development and innovation in Armenia.** The **Ministry of Economy (ME)** oversees industrial policy, supported by key agencies like the **Enterprise Incubator Foundation** and the **Small and Medium Entrepreneurship Development Centre of Armenia**. **The National Centre of Innovation and Entrepreneurship**, under the ME, facilitates idea generation, though its activities are mostly seminar-based due to resource constraints. The Intellectual Property Agency, the National Institutes of Standards, and the National Institute of Metrology under the ME also contribute to the innovation policy system. The Enterprise Incubator Foundation is pivotal in IT development, operating technology centers in Gyumri and Vanadzor. The SME DNC primarily supports small businesses with information services, training, and credit guarantee schemes. **The SDG National Innovation Lab**, a joint initiative between the Armenian government and the UN, aims to accelerate SDG implementation. With the formation of the **Ministry of High Technology Industries**, there is an increased emphasis on technology development and dissemination coordination across ministries. The Ministry of High Tech-Industry is the central body of executive authority. Develops and implements the Government's policy in communication, information, information technology and information security, digitalization, licensing, and military industry.

3.4. Science Funding

18. **Institutional funding provided by the government to research and educational organizations varies across countries. It typically comprises both non-competitive and competitive funding. The state budget allocation for research can be divided into non-competitive and competitive funding, depending on the funding system.** Institutional funding for research usually consists of the following components: **Block grant:** This is a fixed sum, or a proportion of the institutional funding budget allocated to a specific research organization. It is often historically determined with no specific conditions. However, in some cases, it may be linked to a 'performance agreement' between the research organization and the responsible government body. This agreement outlines long-term strategic targets for development negotiated between the parties. **Formula funding:** This portion of the institutional funding budget is determined by specific indicators, such as the organization's size (e.g., number of Ph.D. students, study programs, staff, etc.) and its role in the R&D system. Both research and educational activities influence the level of formula funding. **Performance-based research funding (PBRF)** is a portion of the institutional

[98] See [http://hesc.am/files/1195.pdf], [https://www.e-gov.am/u_files/file/decrees/varch/GVE5-AD2A-6BAF-518F/1195.1.pdf].

funding budget dedicated specifically to research. It is determined by indicators assessing the organization's performance, including research output quantity, research quality, relevance for innovation and society, etc. The proportion influenced by these indicators varies from country to country. **In addition to the mentioned forms of institutional funding, there are other potential types:** Organizations may receive supplementary non-competitive funding for acquiring and maintaining scientific equipment or other infrastructure. Universities may obtain distinct 'teaching funding' as a separate source of institutional income from research funding. This teaching funding is typically determined by specific indicators, such as the number of students, graduates, professors, etc.

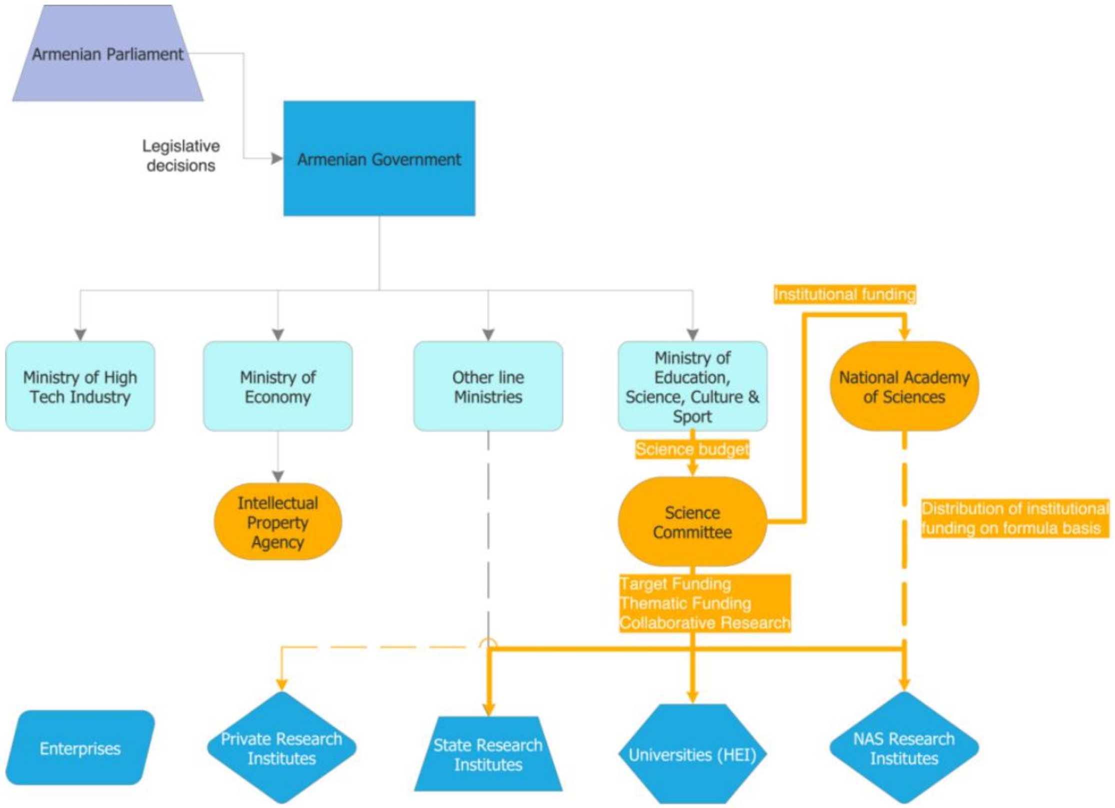
19. **In Armenia, government research funding is managed by the State Committee of Higher Education and Science (SC) through four main financing mechanisms:** 1) Financing the maintenance and development of science infrastructure (about 60% of the total budget) which is allocated to State-owned research institutes; 2) Special-purpose R&D, such as defense-related projects (about 11%); 3) Thematic funding based on calls for proposals from the research community (about 7%); 4) A small portion for collaborative and applied research (less than 1.5%).[99] In 2018, the funding distribution was as follows: Basic or 'institutional funding,' which includes premiums for individuals with a scientific degree, accounted for 73%. Funding for state programs or 'target funding' made up 18%. Contract-based research or 'thematic/topic financing' comprised 9%.

20. **The funding provided by the SC is divided between institutional funding (covering fundamental and applied research, maintenance and development of research infrastructures, support to PhD students and ‘bonus’ payments to scientists with academic degrees) and competitive grant funding. None of these funding streams are directly tied to institutional performance, although expected research outputs are considered in funding requests.** Applications from individual researchers are assessed on a competitive basis by independent experts or a board, though this doesn't constitute a Performance-Based Research Funding (PBRF) system. The SC's process for selecting applications under national grant programs, with the support of a 'professional expert commission,' was established in 2010. This system involves randomly selected experts evaluating factors like research interest, team, and project management. The average expert assessment contributes to 85% of the final score, while an Expert Commission's review accounts for the remaining 15%. Basic funding is distributed by the National Academy of Sciences to Research Institutions per capita, disregarding cost disparities in different scientific fields. This approach limits competitive incentives for attracting and retaining top researchers. The lower salary rates for research roles and the absence of post-doctoral funding were identified as factors negatively impacting the motivation for pursuing a research career.[100]

[99] See supra note 5.

[100] See supra note 4.

Figure 1: Armenian R&I Governance System and Funding Streams



Source: authors

21. **Armenia's gross expenditure on R&D (GERD) has remained largely unchanged as a share of gross domestic product (GDP) in the last decade, at roughly 0.2%.** It has risen in absolute terms to AMD 14 billion (or €25.4 million) in 2018, of which 88.2% was performed in the government sector and 11.8% in higher education. No data is collected on business R&D expenditure. In budgetary terms, government expenditure on science grew between 2013 and 2017; however, the real value is declining given inflation rates. According to the medium-term expenditure framework plan (2019-2021), the annual science budget remained at AMD 14.3 billion (or €25.1 million) for 2019 and the next two years.

Considering GDP growth forecasts, the R&D expenditure share in GDP will decrease further.[101]

22. **The business enterprise sector in Armenia lacks official statistics on R&D expenditure; however, experts generally agree that foreign companies, especially multinational corporations, and a few larger domestic firms in mining, IT, and precision engineering are the major players in business R&D.** Several Armenian start-ups have made their mark in the IT industry, with Picart being one of the most successful. This start-up has received USD 35 million in capital, including funding from Sequoia. Another Armenian start-up that has gained international recognition is BetConstruct, which offers award-winning technology and services for online and land-based gaming. The industry has also seen some major acquisitions, such as Monitis being acquired by GFI Software in 2011, VMWare acquiring Integrien for around USD 100 million, and Oracle acquiring LiveLook to establish a regional R&D hub. The industry has attracted global brands like Synopsis, which has moved a significant portion of its R&D functions to Armenia. With foreign enterprises making up 35% of the country's Information and Communication Technologies (ICT) operations, Armenia has become highly internationalized with significant exports. The engineering sector, especially precision engineering, has shown notable progress in recent years, though it is still relatively small compared to the IT industry, with about USD 25 million in 2015. Global firms' presence and successful operations like National Instruments and IBM signal growth prospects for Armenia. Furthermore, the state's forward-looking development strategy, part of Armenia's 'Export-led Industrial Strategy,' aims to attract multinational production and R&D units, positioning Armenia as a hub for research and development, encouraging growth.[102]

23. **The Armenian research funding system lacks economic incentives for institutions to excel. This hinders overall system development, as there is little motivation for improvement. The available research programs also offer inadequate resources for researchers to establish a strong research profile and pursue their interests.** As a result, while showing promise in some areas, the Armenian research system remains stagnant. Institutions are more inclined to protect this status quo, as it provides a safer way to secure funding than advocating for systemic changes, which come with inherent risks.

3.5. Laws and Regulations Related to Research Security

24. **Recently, Armenia has not implemented any new policies or strategies for research and education. The current policies that govern the science sector in Armenia are the "Strategic Program of Development of Science Sector of the Republic of Armenia in 2017-2020 (SP)" and the "Development Program of the Republic of Armenia's**

[101] See supra note 5.

[102] Two prominent Armenian venture capital firms, Granatus Ventures and Smartgate, provide funding opportunities for Innovative SMEs. Granatus Ventures, established in 2013 with assistance from the Armenian diaspora and the World Bank, focuses on later-stage companies. On the other hand, Smartgate is a privately funded venture capital firm that targets smaller-scale companies, offering financing of up to EUR 85,000. Since late 2014, Armenian start-ups have received USD 87.6 million in funding through venture capital and grants. This funding includes USD 2.1 million in grants from the World Bank and EU/GIZ via the Enterprise Incubator Foundation, which supported 55 deals involving 50 companies. Additionally, there were USD 20.5 million in seed investments across 39 deals with 24 companies, USD 45 million in series A deals across six deals with 5 companies, and USD 20 million in series B deals specifically for the PicsArt company. These investments have significantly contributed to the growth and development of the Armenian startup ecosystem.

Scientific and Technical Field for 2015-2019 (decision N 54 on 25.12.14)" (DP). The SP aims to promote excellence in scientific and scientific-technical activities and create a competent scientific research system to compete internationally, primarily in the European Research Area. The program has several objectives, including improving the science and technology management system, introducing an efficient system for the reproduction of personnel engaged in scientific work, modernizing science infrastructures, promoting fundamental and applied research, and establishing preconditions for a synergistic system of education, science, technology, and innovation. Additionally, the program seeks to develop international scientific cooperation and ensure a smart specialization platform in ERA. Furthermore, DP prioritizes several fields, including Armenology, life sciences, efficient and safe energy, key enabling technologies (such as nanotechnology and biotechnology), IT and communication, space, earth, and nature sciences, and fundamental research. These fields aim to protect national interests, improve the quality of life, raise the economy's competitiveness, ensure sustainable use of natural resources, and manage disasters. The ultimate goal is to boost scientific progress, create high technologies and their usage, innovation development, and civil society.

25. **Several laws and other normative legal acts regulate the research sector in Armenia.**[103] Those include the Law "On Scientific and Technical Activities" (2000 and amendments), Law "On Scientific and Technical Expertise" (2015 and amendments), Law "On State Support For Innovation Activity" (2006 and amendments), Law "On the National Academy of Sciences of the Republic of Armenia" (2011 and amendments), Civil Code of the Republic of Armenia (1995 and amendments), Law "On Education" (1999 and amendments), Law "On Copyright and Related Rights" (2006 and amendments), Law "On Patents" (2022 and amendments), Law "On Higher and Postgraduate Professional Education" (2004), Law "On Foundations" (2002 and amendments), Law "On Non-governmental organizations" (2001 and amendments), and Law "On Control over Export of Dual-Use Items, their Transit through the Republic of Armenia, and Transmission of Dual-Use Information and Results of Intellectual Activity" (2010 and amendments), etc.

26. **The Law "On Scientific and Technical Activities" emphasizes the crucial role of science in economic development, national security, education, culture, and social progress, placing it under state protection. The law aims to regulate various aspects of scientific and technical activities, including legal status, policy objectives, governing body powers, and the status of scientific organizations.** It also guarantees economic, social, and legal freedoms for these activities. Research bodies, including state bodies, public organizations, foundations, or commercial entities, can take various legal forms. A scientific organization can be a commercial or non-commercial legal entity. Meanwhile, a scientific state organization can be a non-commercial, non-profit entity. The law defines scientific activities, such as basic and applied research and experimental developments. It also outlines innovative activities aimed at using scientific results and improving product quality and cost-effectiveness. The state's scientific and technical policy is a component of overall state policy, guiding the activities of state bodies in this domain. The government establishes types of scientific state organizations, sets requirements for their structures, and defines classification criteria, including expected activity results.

[103] See [http://www.scs.am/am/4b52fc7d6382b8c476849619].

27. **The Law "On the National Academy of Sciences of the Republic of Armenia" outlines the functions and status of the National Academy of Sciences of Armenia. It primarily focuses on uniting affiliated research bodies and coordinating fundamental research within Armenia.** The Academy holds a special status as the highest scientific organization in Armenia, functioning as a self-governing, non-profit organization. The Academy possesses rights akin to those of an authorized state governing body for issues assigned to it, enabling it to oversee scientific organizations, legal entities, and institutions within its system. It also has the authority to manage property and exercise rights on its own behalf and is entitled to funding specified in the state budget in a separate line and has its own balance. Furthermore, the Academy serves as an official advisor to the Government on scientific matters, and its proposals hold weight in governmental and administrative considerations. It evaluates normative legal acts related to science. The Academy's structure includes members with varying levels of academic distinction, divisions, staff, and government-founded organizations. Scientific and technical organizations, publishing houses, and institutions operate within the Academy's system. These organizations are established as state non-profit entities by the Republic of Armenia, and the Academy is responsible for their governance. Some scientific organizations in the Academy's system may engage in business activities as allowed by law. Additionally, establishing Academy institutions in foreign countries follows the host country's laws or international treaties involving Armenia. The founder of these institutions is the Academy itself.

28. Other laws relevant to the sphere are the **Law "On Education"** and the **Law "On Higher and Post-Graduate Professional Education."** The latter requires state and private universities to obtain state licensing, with licensing procedures and requirements regularly updated by the MESCS. State funding of research is subject to **the Law "On State Support of Innovative Activities."** The Law "On State Support of Innovative Activities" regulates state funding for research.

29. **The National Strategy of the Republic of Armenia (2020) (the "Strategy")**[104] **highlights that cyberattacks against information resources by foreign states, international terrorist organizations, criminal groups, and individuals threaten Armenia's information security. It further states that private entities pose new and unique challenges, including foreign state-funded cyberattacks targeting Armenia's critical information infrastructure and government structures.** This strategy document includes two relevant sections, *"Ensuring Open and Safe Information and Cyber Domains"* and *"Directing Intellectual Potential towards the High-Tech and Defense Sectors."* It states that the evolving nature of security threats often involves hybrid warfare encompassing military, economic, cyber, and informational elements.

30. **The *"Ensuring Open and Safe Information and Cyber Domains"* (sections 7.9-7.16) further emphasizes that in the modern world, information wars, including propaganda, manipulations, fake news, and other disinformation tools, are becoming more prevalent and often target democratic values.** In this context, the document states that Armenia will work to raise public awareness and media literacy to strengthen the capacity of society and the state to counter such information wars.[105] Armenia lacks a

[104] See [https://www.mfa.am/filemanager/security%20and%20defense/Armenia%202020%20National%20Security%20Strategy.pdf].

[105] See [https://drive.google.com/file/d/1J-IsxkqsWOJ8YhmKTnizWtu6-vKadGXe/view].

comprehensive state policy regulating the information and cybersecurity sector, legislation to protect critical information infrastructure, the insufficient institutional capacity of computer emergency response teams, and a national cybersecurity center. Armenia is committed to developing state information, technological, and cybersecurity policies and strategies and introducing comprehensive mechanisms for the sector's management. Pursuant to the strategy, Armenia commits to developing a legal-normative framework to regulate the relationship between critical information infrastructure operators, digital service providers, and the state. Armenia commits to developing national information and cyber capabilities by effectively managing risks, developing qualified professional potential, localizing international standards, and increasing digital literacy to increase resiliency in the information space. Given the diversity of players, the absence of international borders in the information space, and the involvement of private and public actors in various capacities, it is crucial to increase cooperation between the public, private, and international sectors.

31. **The *"Directing Intellectual Potential towards the High-Tech and Defense Sectors"* (sections 7.36-7.39) emphasizes the targeted use of intellectual resources in the high-tech and defense sectors.** The transformation of the public scientific-educational system into a high-tech hub is a key goal. This restructuring promotes excellence in dual-use technologies, enhancing competitiveness and overall security. The commitment is to ensure equal opportunities and socio-economic inclusion for diverse social groups. Strategic alignment of education and science with state, private sector, and global needs is crucial. The state aims to strengthen the Armenian high-tech sector domestically and internationally through mechanisms that attract public, private, and foreign investments. A major priority is the development of the military-industrial complex, seen as vital for boosting the Armed Forces, driving economic growth, and advancing technology. This involves significant state investments, implementing contracts, encouraging private investment, and expanding production. Incorporating cutting-edge technologies aims to reduce reliance on imported weaponry, markedly increasing the competitiveness of domestically produced military and high-tech equipment globally.

32. **Another relevant field to research security is export control. Armenia is not part of international export control regimes due to its limited production of dual-use or military items, which makes membership less relevant to its economic profile. Nevertheless, Armenia strongly supports the goals and principles of these regimes.** The country is focused on enhancing the efficiency of national mechanisms for controlling dual-use goods. This is governed by the RA Criminal Code and the Law "On Export Control of Dual-Use Items and Technologies and their Transit across the Territory of the Republic of Armenia," enacted on May 15, 2010. The Ministry of Economy is the authorized body for dual-use export control. Additionally, the government has decrees specifying the lists of dual-use items and military products for control and licensing purposes. These measures align Armenia with international agreements on non-proliferation and export control.[106]

[106] See [https://www.mfa.am/en/non-proliferation-strategic-export-control-and-nuclear-security/].
Armenia is not a member of the international export control regimes: Missile Technology Control Regime (MTCR), Nuclear Suppliers Group (NSG), Zangger Committee, the Australia Group, and the prime reason is that Armenia is not a major producer of dual-use items or military goods, materials, and technologies, and the membership in the mentioned regimes may not be relevant to the economic profile of the country. However, Armenia is firmly committed to the goals

33. **The Law "On Export Control of Dual-Use Items and Technologies and their Transit across the Territory of the Republic of Armenia" outlines the requirement for inter-organizational compliance programs, encompassing organizational, administrative, and awareness-building activities to be conducted by exporting entities to ensure adherence to legal turnover control norms within their organizations.** The law defines "controlled items" as those primarily used for civilian purposes, possessing characteristics enabling potential military or weapons of mass destruction application. This also includes "controlled intangible values," encompassing information, intellectual property, and software with similar characteristics that are used for civic purposes and, according to their characteristics and peculiarities, can also be used for military purposes, as well as for developing a weapon of mass destruction and its delivery system thereof. (Article 2). **Under this law, violations of intangible value transmission procedures hold individuals accountable only if they were aware of the item's potential dual-use nature or should have been aware.** Entities engaged in the export of controlled items and the transmission of controlled intangible values must ensure compliance with the regulations outlined in turnover control-related legislation by implementing established internal compliance programs. These internal compliance programs guarantee that entities exporting controlled items and intangible values comply with the regulations outlined in turnover control-related legislation. The governing body offers informational and methodological support to exporting entities in selecting the appropriate tools for implementing these internal compliance programs (Article 8).

3.6. Conclusions

34. **Currently, Armenia lacks a specific government strategy or policy addressing research security. Limited initiatives, training, or awareness programs have been undertaken, with only one workshop held in April 2023 by Sandia National Laboratories, funded by the U.S. Department of State.** However, ongoing reform efforts discussed in this report, including bridging the gap between the public research and higher education R&D systems, enhancing the role of NAS, establishing a national evaluation process that will assess all research institutions every five years to help prioritize government funding, and linking research funding to performance to ensure its effectiveness, provide a foundation for potential improvements.

and principles of these regimes. Armenia pays great attention to increasing the efficiency of the national mechanisms for the control of dual-use goods. The domestic legal system includes the RA Criminal Code and **Law "On Export control of dual-use items and technologies and their transit across the territory of the Republic of Armenia**," adopted on May 15, 2010. The law aims to ensure the fulfillment of Armenia's obligations under international agreements on the non-proliferation of weapons of mass destruction and their means of transportation, as well as in the field of export control. According to the law, the Ministry of Economy of the Republic of Armenia has been recognized as the authorized body of export control of dual-use goods and technologies. The Government Decree N 1785-N adopted the list of dual-use items on December 15, 2011. The European Union's Dual-Use Export Control list was taken as a basis for the national list, and it is periodically being updated and brought to conformity with the EU list. Government decree N 1308-N, "On approving the list of military products, the procedures for licensing import, export, transit of military products, the brokerage in trade of these products, and the formats of the appropriate documents," was adopted on November 12, 2009. According to the Decree, the Ministry of Defense of the Republic of Armenia has been recognized as the authorized body in export control of military products. Government decree N 808-N, "On approving the list of sensitive goods transported from the Republic of Armenia and through the Republic of Armenia", adopted on May 25, 2023.

35. **It is worth mentioning that EU countries' standards and models will likely be more compatible with the country's context and operational capabilities.** Based on our assessment, Armenia is aligning its research and higher education system with the European Research Area, which should inform a reform of research security. Besides, adopting EU standards for research security could help attract Horizon Europe funding/partnerships and partnerships with US research institutions.

36. **The government's National Security Strategy acknowledges the growing threat of information security breaches from foreign entities. This shows the government's dedication to creating legal and institutional cybersecurity frameworks. However, there is no specific provision or mention regarding research security, and no action has been taken in this context.** However, when the government sets information security standards for public and private organizations, it will also be an opportunity for universities and research institutions to enhance their research security.

37. **The current export control laws mandate exporters to establish an internal compliance program encompassing controlled goods, including intangible assets and information, such as research. However, research institutions presently lack these programs**. Although the law mandates liability for failure to comply, which includes implementing internal compliance programs, there is a lack of evidence suggesting universities or research institutions have faced any penalties or consequences. Therefore, it is essential to establish, educate, and enforce these programs within these institutions.

38. **While practical implementation details were not surveyed, informal consultations with university personnel reveal varying levels of information security measures in place, the need for enhanced practical application, and awareness given Armenia's extensive international collaborations.** This report does not delve into the granular details of practical implementation on the ground (formal surveys were not conducted); insights from informal consultations with university personnel unveil a spectrum of information security measures in place. Some institutions have instituted policies on research integrity, intellectual property, and technology transfer. However, it is imperative to acknowledge that **these policies often remain largely theoretical.** Communication with staff is inconsistent, and training and awareness campaigns concerning threats from foreign interference or unauthorized access to critical information and research findings- issues that could potentially affect national security - are largely underemphasized.

39. **Adherence to international best practices in research security will enhance Armenia's global standing. It demonstrates a commitment to the highest ethical and operational standards, reinforcing the country's reputation as a responsible and credible partner in the global scientific community.** Lastly, a clear research security policy and practices will catalyze talent retention and attraction. Local and international researchers are likelier to contribute their expertise to a secure and well-protected research environment. This, in turn, will foster a vibrant knowledge creation and dissemination ecosystem. Establishing research security policies and practices is a safeguard against potential risks and an investment in Armenia's future as a knowledge-driven, innovative nation.

3.7. Recommendations

40. **We emphasize the need for a comprehensive assessment of research security practices** within Armenian Research Institutions (RIs) and Higher Education Institutions (HEIs) informed by this report and the attached questionnaire (Appendix E), as well as an assessment of research funding processes and practices. This has to be done in collaboration with the Ministry of Education, Science, Culture and Sport. We also underscore the value of utilizing the extensive charts detailing potential actions and initiatives employed by leading nations and those proposed by multilateral organizations outlined in the attached (Appendices A, B, C).

41. **Our primary recommendation for this stage focuses on awareness-raising efforts. We encourage the government to establish resources to promote awareness, facilitate dialogue, and share information on research security and integrity among all stakeholders.** Establish forums to promote dialogue and information sharing between the government and the research community. These forums can help identify current and emerging risks, understand the research community's needs, and develop policies to support research security and integrity. Relevant activities may include disseminating reports and studies and organizing seminars, workshops, and stakeholder meetings on various research integrity topics, security risks, and measures. A key aspect is to harmonize integrity principles with security measures, leveraging the existing solid understanding and implementation of research integrity policies among stakeholders while recognizing the need for a dedicated focus on research security practices. This alignment aims to streamline and enhance the implementation process and identify and share information on which research areas are at risk.

42. **To assist in an effective awareness-raising campaign, we recommend the government identify and share information on which research areas are at risk.** It requires collaborating with funders, institutions, and researchers to ensure accurate identification of sensitive, at-risk areas and meet the needs of the research sector. It also requires helping the research community understand the risks in certain areas with a clear link to advancing military or intelligence capabilities, dual-use areas that have both military/intelligence and civilian applications, with significant economic benefits, with access to sensitive personal data or large data sets that may be sensitive in aggregate form, critical infrastructure areas, and/or areas aligned with national economic or strategic interests.

43. **We also advocate for establishing a government-led working group** encompassing all stakeholders tasked with crafting a strategic policy document or conceptual framework outlining specific directions and activities in establishing research security practices.

44. **Informed by this report, we recommend assessing the funding agency's processes and requirements,** ensuring they have disclosure and conflict of interest/ commitment requirements for institutions and researchers. Enhancing the funding agency's capabilities in managing these processes is important.

45. **Informed by this report, we strongly advise collaborating with Higher Education Institutions and Research Institutions to institute an internal compliance program for export control, ensuring strict adherence to legal requirements.** Conduct a pilot internal compliance program with Yerevan State University. Offer training and workshops on creating and implementing these programs.

46. Suggest changes to relevant laws and regulations to ensure they are effectively enforced if needed. Provide comprehensive training and ensure that authorities are actively enforcing the laws.

47. Our additional recommendations are provided in Table 5 below.

Table 5. Additional Recommendations

Additional Recommendation	Action Items
Integrate research security considerations into national and institutional frameworks for research integrity.	• Security and risk management should be integrated into institutional culture and processes as an essential aspect of research integrity. To help achieve this, governments, funding agencies, research institutions, universities, and academic associations can, for example, organize dedicated workshops or develop education and training programs. • Expand the remit of national research integrity offices, where these already exist, or may wish to establish a dedicated national contact point or center of expertise for research security within the government to work with counterparts across the research ecosystem.
Promote a proportionate and systematic approach to risk management in research.	• Science and security agencies need to develop trusted processes that ensure regular information exchanges and promote mutual understanding of the benefits and risks of international collaboration. • The governments should encourage responsible self-management (self-policing) by universities and professional associations and support capacity building to better understand, identify, and mitigate potential risks. • The government funding agency, research institutions, and universities must regularly assess the maturity of their security strategies and adjust policy initiatives or actions to ensure effectiveness. It is important to monitor for unintended consequences, including discrimination against specific population groups and ethnic profiling or reductions in research collaborations.
Promote openness and transparency about conflicts of interest or commitment.	• The government should collaborate with research providers, including universities, to raise awareness of research security issues and communicate what information research providers and researchers are required or expected to provide. • Funding agencies, research institutions, and universities must establish clear and transparent systems to ensure researchers declare information about conflict of interest or conflict of commitment and potential research security risks. Checklists or toolkits can be helpful resources to guide the risk identification and mitigation process. • Universities, research institutions, and individual researchers should implement transparent processes to ensure due diligence when establishing research partnerships. In addition to assessing the risks for new projects, ongoing projects must be monitored.
Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy.	• New procedures for ensuring research security may be required, but as far as possible, the procedures should be harmonized with existing procedures or structures. • Universities and research institutions should establish transparent processes to help researchers navigate the policy landscape and minimize the burden of new regulations and guidance. Engaging researchers in the development of policies can help improve their effectiveness.

Additional Recommendation	Action Items
Work across sectors and institutions to develop more integrated and effective policy.	• Establish coordination structures that unite ministries or departments interested in research security. Such structures can play an important consultation and communication role and advise on and monitor relevant policy initiatives. • Ministries or agencies responsible for education, science, and innovation need to facilitate collaboration and exchange of information among the different actors in the research ecosystem (funding agencies, research institutions, universities, and the academic research community) while at the same time liaising closely with other governmental bodies. • Research institutions and universities should share information on research security issues and the cases they are confronted with, both within and with other research institutions and stakeholders in the research ecosystem.

APPENDIX A. CHART ON RESEARCH SECURITY POLICIES AND INITIATIVES

NATIONAL GOVERNMENTS			
Country	**Policies and Regulations**	**Guidance**	**Sharing of Information between Stakeholders**
United States	The 116th Congress in 2021 passed legislation mandating the disclosure of funding sources in federal research and development awards applications. The U.S. Government issued a presidential memorandum to enhance cooperation between law enforcement and funding agencies, focusing on safeguarding government-supported research.	The U.S. Government released Recommended Practices for enhancing the security and integrity of science and technology research, including establishing organizational policies for conflicts of interest, standardizing disclosure requirements, providing training on responsible research conduct, and enforcing consequences for non-compliance.	The Presidential Memorandum on United States Government-Supported Research and Development National Security Policy, issued by The White House in 2021, mandates the Director of the Office of Science and Technology Policy (OSTP), in collaboration with the Director of National Intelligence (DNI) and relevant agency heads to engage with the U.S. research and development (R&D) community. The goal is to heighten awareness of research security and integrity risks and establish policies and measures for addressing these risks.
United Kingdom	The National Security and Investment Act grants the national government authority to intervene in specific acquisitions that may threaten the UK's national security. The Academic Technology Approval Scheme (ATAS) in the United Kingdom applies to international postgraduate students studying certain sensitive subjects.	The Centre for the Protection of National Infrastructure published Trusted Research Guidance for Academia, focusing on maintaining integrity in international research collaboration. It specifically targets critical areas like STEM subjects, targets critical areas like STEM subjects, emerging technologies, and commercially sensitive research. The UK Export Control Joint Unit issued guidance on export controls for academic research. The UK Government established a Research Collaboration Advice Team (RCAT) to offer guidance on safeguarding research from hostile activities during international collaboration. The advice covers export controls, cyber security, and intellectual property protection.	The Centre for the Protection of National Infrastructure (CPNI) conducts workshops in partnership with the academic sector to assist universities in managing national security risks related to research. These workshops help scholars identify and address risks and security concerns in international research collaborations. Additionally, the CPNI STEM Universities Forum was established to facilitate confidential information-sharing on secure research collaboration among UK STEM research-intensive universities, CPNI, the National Cyber Security Centre, and, as appropriate, government and arm's-length bodies.
Canada	Individual researchers must evaluate potential national security risks associated with international collaborative projects. The National Security Guidelines for Research Partnerships identify sensitive or dual-use research areas requiring particular attention.	The Canadian government released a Policy Statement on Research Security and COVID-19, encouraging awareness of potential risks and urging protective measures while upholding Open Science principles. National Security Guidelines for Research Partnerships were introduced to prevent interference, espionage, and knowledge transfer that could benefit entities threatening	Canada has established the Government of Canada-Universities Working Group brings together universities, government departments, federal granting councils, and national security agencies. The group's objective is to advance open and collaborative research while safeguarding research and maximizing benefits for Canadians. At the operational level, the

NATIONAL GOVERNMENTS			
		Canada. These guidelines apply to federal research partnership funding. Online courses, "Introduction to Research Security" and "Cyber security for researchers" was created to train researchers and university staff.	Natural Science and Engineering Research Council's (NSERC) Alliance Grants support this initiative.
Japan	Technology transfers within Japan's domestic transactions are not categorized as exports. However, the national government has initiated oversight of sensitive technology transfers between domestic residents whom foreign governments or companies may influence. Residents receiving substantial financial benefits or contracts (e.g., employment contracts) from foreign entities are deemed potentially influenced by them.	Japan implemented policy directions to ensure research integrity, necessitating researchers to report foreign financial support and affiliations to their institutions and funding agencies. Failure to report may result in bans on future research funding applications.	
Australia		The University Foreign Interference Taskforce (UFIT) was established to counter foreign interference in the Australian university sector. It provides guidelines covering governance frameworks, due diligence, communication, and education on risk and cyber security.	The University Foreign Interference Taskforce, a joint initiative of the Australian Department of Education, Skills, and Employment and the Department of Home Affairs, has developed Guidelines to Counter Foreign Interference in the Australian University Sector. These guidelines were formulated through collaborative efforts involving a steering group and working groups with representatives from universities and government agencies.
The Netherlands		The Netherlands is developing guidelines, checklists, and self-evaluation tools for research institutions and universities to protect knowledge security in international collaborations. They aim to prevent unauthorized knowledge, technology transfer, and covert influence by state actors.	
New Zealand		The government developed Trusted Research Guidance for research institutions, universities, and researchers, incorporating an analysis of existing legislation relevant to research security.	

FUNDING AGENCIES			
Country	**Guidelines and Regulations**	**Managing Conflicts of Interest or Commitment**	**Risk Assessment and Management**
United States	The U.S. National Science Foundation (NSF) has prohibited its staff from participating in foreign government talent recruitment programs. They have established a position dedicated to research security strategy and policy, tasked with developing and implementing strategies to enhance research security and improve coordination with other federal agencies.	The U.S. Government Accountability Office (GAO) in 2020 recommended that funding agencies establish written procedures for handling instances where required information, like foreign affiliations, is not properly disclosed. These procedures should detail the steps of the investigation process, assign specific roles and responsibilities, and specify potential administrative or enforcement actions if allegations are confirmed. Funding agencies have various options, including requesting the researcher's university to initiate an investigation, temporarily suspending grants, or referring cases for legal prosecution.	The U.S. Department of Energy (DOE) has established a Science and Technology Risk Matrix to pinpoint areas of critical emerging research that lack regulatory control mechanisms but may necessitate additional protective measures due to their national or economic security implications. DOE utilizes this Risk Matrix to inform and guide decisions regarding international engagements.
United Kingdom	UK Research and Innovation (UKRI) provides clear expectations for the conduct of research it supports through funding policies and terms and conditions. They are reinforced by guidance and an active funding assurance or audit program. UKRI has also outlined principles regarding due diligence for international collaboration, although they do not actively monitor compliance, respecting the autonomy of research organizations.		Various UK research councils and the Wellcome Trust incorporate a question on grant application forms that prompts applicants to consider the short and medium-term risks of misuse associated with their proposals. They also guide risks of misuse to external experts who review grant applications. The application may not receive funding if serious concerns about potential misuse arise and cannot be addressed through agreed-upon management strategies with host institutions. Researchers are expected to promptly inform funders and host institutions of any newly emerging risks related to dual-use research of concern that may not have been identified during the grant application process.
Norway	Projects funded by the National Research Council in Norway operate under a contract. This contract mandates project managers to adhere to applicable laws, ethical guidelines, and recognized quality standards and norms for good research practice.		
Portugal	In Portugal, an administrative law mandates a declaration of conflicts of interest (COI) for all individuals involved in the grant review process. This measure helps ensure transparency and integrity in the evaluation of grants.		
Canada			Applicants to the Natural Science and Engineering Research Council’s (NSERC)

FUNDING AGENCIES			
			Alliance Grants Program, a federal research funding partnership, must complete risk assessment questionnaires. If any risks are identified, applicants must develop plans to mitigate those risks. The funding agency then reviews risk assessment questionnaires and mitigation plans before making funding decisions.
Germany			The German Research Foundation (DFG) and the National Academy of Sciences Leopoldina have jointly developed guidelines to minimize misuse risks and support self-regulation by individual researchers, research institutions, and universities. These guidelines recommend that individual researchers conduct risk analyses, take steps to minimize risks, responsibly publish sensitive results, and refrain from research with a high risk of misuse. Research institutions and universities are advised to establish ethical rules for handling security-relevant research and adhere to legal regulations. Additionally, the DFG includes considerations for handling security-related aspects of research projects in its application guidelines. Applicants must assess whether their proposed projects involve immediate risks of dual-use, and if so, they must provide a risk-benefit analysis and describe measures to mitigate those risks. If the applicants' research institutions or universities have research ethics committees, these committees must be consulted in advance, and their statements need to be included in the research proposals.

INSTITUTIONS AND ASSOCIATIONS			
Country	**Public Research Institutions**	**University Associations**	**Academic Associations**
United States	The U.S. Department of Energy (DOE) has a policy prohibiting its employees and contractors from simultaneously working within the DOE complex while participating in specific foreign government-sponsored talent recruitment programs or engaging in certain foreign government-sponsored or affiliated activities.	APLU and AAU: Released a report in 2020 on "University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus." This report surveyed practices universities employ to ensure research security, protect against intellectual property theft, and prevent foreign government influence or actions infringing on academic values. It also emphasizes fundamental principles and values, including academic freedom, free expression, diversity, and transparency.	National Academies of Sciences, Engineering, and Medicine: Launched the National Science, Technology, and Security Roundtable in 2020. This roundtable brings together experts from various fields, including research agencies, national intelligence, law enforcement, academia, and business communities. It identifies and assesses security risks related to federally funded research and development. Additionally, it works to develop effective communication approaches for conveying risks to the academic and scientific community and shares best practices for risk mitigation. JASON: An independent advisory group of scientists has proposed a series of instructive questions for principal investigators to consider before engaging with foreign research entities. American researchers have adopted these questions as a toolkit/checklist to aid in conducting due diligence when entering into research collaborations.
Germany	The Max Planck Society in Germany recently established new guidelines for its researchers. These guidelines advise researchers to identify and minimize risks related to human rights, academic freedom, and scientific espionage before initiating international collaborations. Additionally, administrative headquarters must approve third-party funds before researchers can accept them. In cases where researchers have questions about rules or policies, an ombudsperson is available to provide them with confidential advice. Similarly, the Leibniz Association mandates its institutions and researchers to assess political situations in partner countries and evaluate the motivations of research partners.	German Rectors’ Conference and German Academic Exchange Service: Formulated guidelines and standards for international partnerships, particularly in joint research. These guidelines focus on principles like freedom of research, adherence to scientific, ethical, and legal standards, equal partnership, and promotion of researcher mobility. They also highlight the importance of ethical and legal standards, including intellectual property protection and handling security-related research.	German Academy of Sciences Leopoldina: Organizes conferences and workshops on the handling of security-relevant research. These events involve experts from various disciplines to raise awareness among researchers regarding the security aspects of their work and provide a platform for sharing experiences. They also facilitate discussions on specific security-relevant research projects and assess whether self-regulated restrictions are adequate to prevent malicious use. The German Academy of Sciences Leopoldina assists research institutions and universities in establishing local committees responsible for ethics in security-relevant research.
United Kingdom		Universities UK – UUK: Published guidelines in 2020 to support universities in managing risks associated with internationalization. These guidelines provide key actions and case studies for governing bodies and executive leaders. They stress the importance of changes in awareness, institutional systems, and cross-sector processes to mitigate international security	UK Royal Society: Provided feedback on the Foreign Influence Registration Scheme (FIRS) during its consideration by the UK government. The Society acknowledged the importance of addressing threats from hostile activities, including theft, misuse, or exploitation of research and the potential loss of personal information. The Society emphasized the need for balanced regulations, highlighting the potential chilling effect overzealous regulations could have on the

INSTITUTIONS AND ASSOCIATIONS			
		threats while maintaining secure partnerships. UUK also recommends considering reputational, ethical, and security risks in addition to financial risks.	academic research community and international collaboration.
Canada		U15 Group of Canadian Research Universities: Published a guide in 2019 on "Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects." This guide offers practical advice and best practices for conducting economic and geopolitical risk assessments and mitigating key risks. It includes checklists and a matrix to assess these risks, covering areas like project team building, assessing non-academic partners, cybersecurity, data management, and international travel.	
Australia	Australia's Commonwealth Scientific and Industrial Research Organization (CSIRO) developed the Research Engagements Sensitivities Tool (REST) in 2020-2021. This tool assesses risks related to foreign interference and facilitates systematic decision-making regarding new research opportunities. The final decision-maker's rank for project approval corresponds to the assessed risk level of the project. In cases where reviewers identify high risks, the CEO must approve any collaboration with new partners. CSIRO has also started sharing its tools and expertise for risk assessment with Australian universities.		
Sweden		Swedish Foundation for International Cooperation in Research and Higher Education – STINT: Developed "Responsible Internationalization: Guidelines for Reflection on International Academic Collaboration" in 2020. These guidelines offer key questions for reflection at various stages of a collaboration, including those related to risks that may affect academic freedom. They serve as a basis for dialogue within and between Swedish universities	

UNIVERSITIES			
Country	**Policies and Guidelines**	**Management and Oversight**	**Research Security Training**
United States	University of Texas at Austin: It aims to establish a transparent system for disclosing, approving, and documenting employees' external activities that could raise concerns about conflicts of interest or commitment. This policy requires researchers to complete a Financial Interest Disclosure and undergo mandatory training. University of Michigan, Rochester University: These universities have developed similar policies focused on ensuring compliance with domestic laws and protecting the freedom of scientific research from illegal foreign interference. Rochester University: Have interim guidelines covering all aspects of research collaboration, whether conducted on campus or abroad. These guidelines mandate disclosing any form of international collaboration and support, such as talent programs, grants, and gifts. To ensure policy adherence, the university closely monitors visitors, including students, faculty, researchers, and short-term visitors.	University of Michigan: Operates a Research COI Committee responsible for reviewing disclosures of outside activities from researchers seeking sponsorship for their research proposals. The committee evaluates whether external activities could significantly impact research design, conduct, or reporting. They aim to ensure that an individual’s interests do not unduly influence their primary obligations to science, research sponsors, the university, colleagues, or students. If COIs are identified, strategies are developed to manage them appropriately.	University of Michigan: Offers comprehensive training in research ethics and compliance through the Programme for Education and Evaluation in Responsible Research and Scholarship. This includes online modules covering research integrity, conflicts of interest, export controls, and research information security. Initially required for federally funded projects, it's now mandatory for all faculty, staff, and students involved in scholarship and research.
Canada	University of Toronto, McGill University: These universities have developed similar policies focused on ensuring compliance with domestic laws and protecting the freedom of scientific research from illegal foreign interference. University of Toronto: Has created a Research Partnership Security Checklist for International Partnerships. This checklist is designed to assist principal investigators in evaluating the suitability and potential risks of engaging with an international partner before commencing a specific project. Principal investigators must complete the checklist within two weeks of submitting research proposals or before initiating international research partnerships.		
Netherlands		Each university in the Netherlands has a Knowledge Security Advisory Team. This virtual team comprises experts in safety risk management, information security, and international collaboration. It can also bring in additional experts for specific research topics, countries, and human resource issues. The	

UNIVERSITIES			
		team assists the university's executive board in making decisions related to knowledge security issues. In cases where a smaller university lacks the necessary expertise to assess knowledge security risks, they can seek assistance from a Knowledge Security Advisory Team at another university.	
Norway			Act on Ethics and Integrity in Research: Mandates that all research institutions and universities provide education in research ethics, including the responsible use of new technologies, to all employees and researchers.
Sweden			Lund University: Requires all Ph.D. students to complete a research ethics course. This course provides a foundation in research integrity and addresses ethical challenges in developing and implementing new technologies.

APPENDIX B. RECOMMENDATIONS BY EXPERT GROUP, GLOBAL SCIENCE FOUNDATION, AND THE OECD-GSF SECRETARIAT[107]

Recommendation	Justification	Action Items
Underscore the importance of freedom of scientific research and international collaboration as a key element of the global research ecosystem	Freedom of inquiry and international collaboration constitute an essential part of scientific research and are enshrined in several international organizations' formal and informal recommendations and declarations. Geopolitical tensions and the behavior of governments can undermine scientific freedom and international collaboration and create real or perceived xenophobia or prejudice.	• Governments should promote international collaboration while taking a proportionate risk management approach to security issues. In this context, international mobility and recruiting foreign researchers should be recognized as essential to international collaboration. • Research institutions and universities should maintain welcoming and inclusive environments where freedom of scientific research and science communication is respected, and everyone is treated equally, regardless of race or national origin.
Integrate research security considerations into national and institutional frameworks for research integrity	As international collaboration becomes more widespread and the geographic distribution of scientific production changes, mitigating unauthorized information transfer and foreign interference needs to be included in research integrity and scientific responsibility considerations.	• Security and risk management should be integrated into institutional culture and processes as an essential aspect of research integrity. To help achieve this, governments, funding agencies, research institutions, universities, and academic associations can, for example, organize dedicated workshops or develop education and training programs. • Countries can expand the remit of national research integrity offices, where these already exist, or may wish to establish a dedicated national contact point or center of expertise for research security within the government to work with counterparts across the research ecosystem.
Promote a proportionate and systematic approach to risk management in research	Risk management needs to acknowledge freedom of scientific research on the one hand and security considerations on the other hand. Policies and actions to address research integrity and security should be based on sound risk identification and assessments and be regularly revisited and revised as necessary. Not every research institution or research project will face the same level or type of risk. Maintaining institutional autonomy in risk management and decision-making is key to effectively identifying risk and gaining crucial buy-in across the research sector.	• Science and security agencies need to develop trusted processes that ensure regular information exchanges and promote mutual understanding of the benefits and risks of international collaboration. • Governments should encourage responsible self-management (self-policing) by universities and professional associations and support capacity building to better understand, identify, and mitigate potential risks. • Governments, funding agencies, research institutions, and universities must regularly assess the maturity of their security strategies and adjust policy initiatives or actions to ensure effectiveness. It is important to monitor for unintended consequences, including discrimination against specific population groups and ethnic profiling or reductions in research collaborations.
Promote openness and transparency about conflicts of interest or commitment	Recognizing and avoiding potential COI and COC while collaborating internationally is not always easy. It is important to clarify requirements for disclosure of potential COI and COC and establish processes that support transparency and help manage risks.	• Governments should collaborate with research providers, including universities, to raise awareness of research security issues and communicate what information research providers and researchers are required or expected to provide. • Funding agencies, research institutions, and universities must establish clear and transparent systems to ensure researchers declare information about COI and COC and potential research security risks. Checklists or

[107] See **OECD Science, Technology, and Industry Policy Papers**, "*Integrity and Security in the Global Research Ecosystem"* June 2022, No. 130.

Recommendation	Justification	Action Items
		toolkits can be helpful resources to guide the risk identification and mitigation process. • Universities, research institutions, and individual researchers should implement transparent processes to ensure due diligence when establishing research partnerships. In addition to assessing the risks for new projects, ongoing projects must be monitored.
Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy	Governments, funding agencies, research institutions, and universities must develop simple, clear, and unambiguous guidelines targeted at specific risks to avoid unnecessarily burdening researchers. National governments and funding agencies should limit additional administrative burdens related to security measures and, where possible, leverage existing processes. Confusing, complicated, and burdensome rules are unlikely to be effective and can hurt research development.	• New procedures for ensuring research security may be required, but as far as possible, the procedures should be harmonized with existing procedures or structures. • Universities and research institutions should establish transparent processes to help researchers navigate the policy landscape and minimize the burden of new regulations and guidance. Engaging researchers in the development of policies can help improve their effectiveness.
Work across sectors and institutions to develop more integrated and effective policy	Different stakeholder actions need to be coordinated effectively for mutual benefit. Research integrity and security are relevant across many government policy areas. At the same time, research integrity and security engage multiple stakeholders outside of ministries, including funding agencies, research institutions, universities, and individual scientists. This complexity can make it challenging to agree on responsibilities and actions to protect research integrity and security.	• Governments can establish coordination structures that unite ministries or departments interested in research security. Such structures can play an important consultation and communication role and advise on and monitor relevant policy initiatives. • Ministries or agencies responsible for education, science, and innovation need to facilitate collaboration and exchange of information among the different actors in the research ecosystem (funding agencies, research institutions, universities, and the academic research community) while at the same time liaising closely with other governmental bodies. • Research institutions and universities should share information on research security issues and the cases they are confronted with, both within their institution and with other research institutions and stakeholders in the research ecosystem.

APPENDIX C. RECOMMENDATIONS BY THE EUROPEAN COMMISSION[108]

Categories	Recommendation	Action Items
Values	a) Identify countries and partner institutions where academic freedom is at risk	• Consult the global Academic Freedom Index (AFi) as a first point of orientation. • Then conduct a more detailed assessment of the research, educational and institutional environment in the country and at the specific partner institution. • Subsequently, analyze the external actors' motives for undermining academic freedom and monitor the external actors' capacities for restricting and/or instrumentalizing European researchers and institutions.
	b) Conduct a vulnerability assessment to understand external pressures on academic freedom and integrity in the institution	• Undertake institution and/or project-specific vulnerability assessments. • Review if existing cooperation with external actors has created any dependencies. • Verify that all partnership agreements adequately protect academic freedom. • Monitor external appointments as well as honorary degrees awarded to researchers. • Provide training to everyone interacting with institutions where academic freedom and universal values are at risk. • Set-up a reporting mechanism to map threats to academic freedom in the institution.
	c) Strengthen commitment to academic freedom and integrity at institutional and individual levels	• Address specific vulnerabilities once they are identified. • Provide training to everyone interacting with institutions where academic freedom and universal values are at risk. • Integrate academic freedom and integrity into the core curriculum of any academic education program. • Affirm frequently and publicly the importance of academic freedom and integrity. • Raise awareness among students, academic and administrative staff for the importance and protection of fundamental academic values. • Support scholars who work on research topics that external actors seek to suppress. • Launch a dedicated support program for visiting scholars and incoming students from countries where academic freedom is threatened. • Help protect persecuted scholars or students by providing (temporary) sanctuary. • Consider signing a democracy pledge.
	d) Continue to cooperate with partners in repressive settings	• Avoid stigmatizing or alienating students, academic colleagues and institutions in non-liberal institutional environments. • Create awareness and understanding of how repressive settings can affect academic freedom. • Review standard ethics procedures to ensure that risky research in repressive settings will not automatically be rejected (and thereby repressed) by the relevant committee. • Provide guidance and tailored technical support on data and digital security to help manage surveillance risks in repressive settings. • Set up an emergency procedure to deal with cases of harassment, detention or disappearance. • Commit to transparency and screening mechanisms tailored to address collaboration with repressive settings.
Governance	a) Publish a Code of Conduct for Foreign Interference	• Ensures protection of academic freedom, data security and intellectual property, excellence and openness in research, teaching, and support for learning, ethics, integrity, and trust. • Include procedures for identification of foreign interference (including data breaches and ethically unsound research); whistleblower protection; dealing with internal conflicts of interest
	b) Establish a Foreign Interference (FI) Committee	• Integrate FI Committee with existing institutional structure and responsible for: - awareness raising through education & training; - monitoring of potential risks; - monitoring of potential risks; - management of research data and intellectual

[108] See **European Commission, Directorate-General for Research and Innovation**, "*Tackling R&I foreign interference – Staff working document*", Publications Office of the European Union, 2022.

Categories	Recommendation	Action Items
		assets in international cooperations and providing advice and support to research groups involved; - risk management and risk mitigation; - investigation of Foreign Interference.
Partnerships	a) Develop general prerequisites for the implementation of a risk management system	• A Foreign Interference Investigation Committee should ensure that knowledge security and academic integrity is safeguarded in all partnerships by reviewing procedures and expanding and strengthening them where needed. • Raise broad awareness of potential risks involved in engaging in a partnership and of the ways the institution seeks to mitigate them. • Raise support for a risk management strategy. • Create awareness and knowledge of export control legislation and Foreign Direct Investment (FDI) screening. • Identify and protect the institution's 'crown jewels' and understand the potential technological, security and economic interests from third countries. • Define criteria for reporting plans for a partnership to the FI Committee and determine who is accountable for following up on the reporting. • Define the minimum levels of due diligence for different types of partnerships. • The Foreign Interference Committee could establish a risk management subcommittee or working group.
	b) Establish a sound procedure for developing robust partnership agreements	• Develop a positive agenda: identify safe or low-risk areas for international collaboration. • Prepare for partnership: ensure it is based on a strategic vision as part of internationalization. • Develop a sound knowledge of the partner organization of its place in the national research system of its country. • Perform due diligence: gather information enabling staff to assess potential risks concerning security, values and reputation.
Cybersecurity	a) Raise awareness of cybersecurity risks	• Develop training and organize seminars on all available and implemented data protection technologies including confidential computing. • Educate and train researchers, students, and administrative and support staff in cyber hygiene and to identify the risks and know how to avoid or deal with cyberattacks. • Develop and communicate easy-to-follow escalation processes in case of suspected cyberattacks and advertise a single point of contact for triaging the reported incidents. • Maintain and communicate a Top 10 cybersecurity risk list. • Publish regular newsletters with best practices describing cybersecurity incidents.
	b) Detect and prevent cybersecurity attacks from foreign interference actors	• Set up and regularly perform Open-Source Intelligence (OSINT) investigations and create alert capabilities to flag outlier behavior. • Develop screening procedures for researchers and administrative and support staff. • Procure cybersecurity-certified equipment and invest in developing confidentiality protection solutions for datasets, including confidential computing. • Implement physical access controls appropriate to the level required. • Develop a centralized management approach for the office/corporate activity cluster for operating systems and installed applications and disable and remove local administration rights (LAR). • Enable two-factor authentication (2FA) to access critical services and repositories and maintain and enforce block lists to prohibit access to known malicious or infringing websites.
	c) Respond to and recover from cybersecurity attacks from foreign interferers	• Develop situational awareness capabilities by sharing lessons learned and updating shared blacklists, reputation systems, and databases. • Develop a plan for incident handling, including clear processes involving affected parties and those required to handle the response. Adopt practices and elements from incident handling models such as the SIM3 Security Incident Management Maturity Model. • Implement forensic readiness capabilities to reduce the time to respond.

Categories	Recommendation	Action Items
		• Follow disciplinary action for offending staff and include evidence from the digital investigation. • Involve relevant law enforcement agencies, national intelligence and security agencies, Intellectual Property offices, and data protection authorities for incidents.

APPENDIX D. RECOMMENDATIONS BY SIGRE WORKING GROUP, G7 COUNTRIES[109]

Recommendations	Government	Research Funders	Research Institutions	Researchers
Establish resources to promote awareness and forums for dialogue and information sharing on research security and integrity across all research stakeholders	**Establish Dialogue Forums** Create platforms for government-research community interaction. Aim to identify current and emerging risks. Understand research community needs. Develop policies for research security and integrity. **Share Information** Disseminate unclassified information to funders, institutions, and researchers. Inform about new risks or practices. Facilitate mutual understanding of research culture and processes with government stakeholders. **Central Resource Hub** Develop a centralized information source for researchers. Provide updated information on emerging risks. Offer guidance on implementing best practices. Equip researchers with resources for effective implementation.	**Promote Research Funding and Programs** Actively participate in disseminating and advocating for research funding and programs. Contribute to the formulation of comprehensive research security and integrity policies. **Raise Awareness through Resource Dissemination** Assist in sharing resources to enhance awareness and understanding.	**Active Dialogues with Researchers** Establishing active dialogues enables the development of tools and resources. Closes gaps in risk understanding. Provides tailored, current information on the risk environment for specific organizational contexts and processes. **Regular Staff Training and Updates** Ensure staff are regularly trained and updated on potential risk areas. Focus on mitigation strategies to keep them informed about existing threats. **Resource Dissemination to Researchers** Share resources with researchers to foster risk awareness within their research community. .	Effective awareness-raising and information-sharing empower researchers to safeguard their research and uphold the integrity of domestic and international research environments. Researchers also play a crucial role in advocating for their needs in dialogues with governments, research funders, and institutions, ensuring that these entities can address them effectively
Identify and share information on which research areas are at risk	**Collaborative Approach** Work closely with funders, institutions, and researchers to precisely identify at-risk areas. Address the specific requirements of the research sector collectively. **Risk Awareness in the Research Community** Assist in educating the research community about risk-prone domains.	**Targeted Implementation of Security and Integrity Requirements** Implement research security and integrity measures specifically focusing on high-risk research areas. **Effective Communication with Researchers** Discuss with researchers to ensure a thorough	**Awareness of Sensitive Research Activities** Institutions should be aware of the research activities conducted within them, especially in areas considered sensitive by the government. **Support for High-Risk Research** Assist researchers in recognizing and addressing higher-risk research by providing relevant information and support.	**Proactive Risk Assessment** Researchers should assess how their work might be misused or misappropriated. **Government Guidance Adherence** They should follow government guidance to ascertain if their research falls under sensitive categories. **Utilize Due Diligence Tools**

[109] See **Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group**, "*G7 Best Practices for Secure & Open Research*", May 2023.

Recommendations	Government	Research Funders	Research Institutions	Researchers
	Emphasize areas linked to military/intelligence advancement, dual-use applications, economic significance, access to sensitive data, critical infrastructure, and alignment with national interests.	understanding of projects and their associated potential risks.		Researchers should use tools provided by governments, funders, or institutions for conducting thorough due diligence on their research activities.
Identify areas of risk activity by conducting due diligence and ensuring transparency and the disclosure of relevant information	**Collaborative Policy Frameworks** Collaborate with research communities to develop policy frameworks that establish transparent and due diligence requirements for funders, institutions, and researchers. These should balance national and global interests while ensuring safeguards against identified risks. **Guidance and Continuous Assessment** Work with national security agencies to regularly guide research institutions and researchers on current risks. Continuously assess the threat environment to ensure the research community is adept at identifying risks and that policy frameworks remain consistent in safeguarding research. **Ongoing Policy Evaluation** Regularly review policy frameworks to ensure they still meet the needs and objectives of research security and integrity. **Monitoring for Unintended Impacts** Share insights on risk identification trends and monitor for unintended adverse impacts of established policy frameworks. Ensure academic freedom is preserved and prevent discrimination and harassment.	**Efficient Risk Disclosure** Utilize government-established regulations or guidance for researchers to easily and transparently disclose and identify application risks. **Standardized Conflict of Interest Disclosure** Consider incorporating requirements for transparency and disclosure of potential conflicts of interest in funding application forms. This includes information on project team members' affiliations, appointments, and any funding from other sources, including foreign governments. **Safeguarding Research Freedom and Preventing Discrimination** Research funders should actively monitor for unintended adverse impacts of their security and integrity programs. They must take corrective action to uphold research freedom and prevent discrimination or harassment within their funding programs	**Capacity Building for Risk Identification and Evaluation** Institutions should establish the capacity to assist researchers in recognizing and assessing risks. This includes ensuring transparency in information disclosure. **Designated Senior Leadership for Research Security and Integrity** Appoint a senior leader to oversee research security and integrity matters. This individual will be responsible for ensuring a consistent approach. They may integrate research security risks into existing frameworks like risk registries or institutional research integrity frameworks. **Regular Discussion of Risks at the Senior Leadership Level** Reputational, ethical, and national security risks related to research projects should be a regular topic of discussion at the senior leadership level. This allows for swift responses to emerging concerns. **Clarity in Risk Management Decision-Making** Ensure that those responsible for risk management understand their roles and have appropriate support. They should know when to escalate decisions to a higher level. **Institutional-Level Risk Identification** Identify and assess risks that apply across multiple projects or research	**Researchers' Expertise in Identifying Risks** Researchers possess in-depth knowledge of their research domain and are best equipped to identify potential risk areas, especially concerning partnerships and individuals. They should be supported by credible risk information from governments and other reliable sources. **Commitment to Risk Identification and Mitigation** Researchers should actively identify, evaluate, and mitigate potential risks to the integrity and security of their research. This involves transparently disclosing pertinent information to their institutions and funders. **Understanding Partner Motivations** Understanding the motivations and interests of partners and team members is crucial in identifying potential risk areas. Due diligence reviews can reveal indicators of compromised autonomy, connections to foreign entities, or operations in countries known for intellectual property theft. **Clear Collaboration Processes** Regardless of partnership formality, having clear, shared, and documented collaboration processes is essential. It supports research integrity by thoroughly understanding all involved parties and their roles.

Recommendations	Government	Research Funders	Research Institutions	Researchers
			areas. This could include infrastructure-based physical and digital risks, typically managed at an institutional level. **Transparent Research Agreements** Institutions should review research agreements to ensure clear documentation of outcomes that benefit all parties involved. **Monitoring for Adverse Impacts** Research institutions should actively monitor the implementation of research security and integrity initiatives to avoid adverse impacts. Any such findings should be reported to relevant funders or governments for immediate action to maintain research freedom and prevent discrimination or harassment.	**Reporting Discrimination or Harassment** Researchers should know that research security and integrity measures should be applied without bias towards specific individuals or communities. Any discrimination or harassment should be promptly reported to institutions, funders, or governments for immediate action.
Implement risk mitigation measures, both as standard organizational practice and for individual research projects	**Create resources and information-sharing balance of the research community in implementing this best practice**	**Incorporate Security and Integrity Requirements** Institutions should consider including specific research security and integrity criteria in their application processes. They may also establish policies or conditions that make certain risk mitigation measures standard expectations for funding. **Training and Cybersecurity Requirements** Encourage or mandate program participants to undergo specific training on research security. They should also have cybersecurity plans and data management controls aligned with evolving best practices in the research community.	**Measures for Protection** Implement various protective measures, including cyber security practices, physical access controls, compliance with relevant legal obligations, and establishment of intellectual property protections. **Code of Conduct for Researchers** Establish a code of conduct on research security and integrity. This sets broad standards and expectations for researchers' behavior, including how to respond to security incidents. Clear reporting policies and processes should be in place to facilitate risk identification and mitigation. **Training on Security Standards** Provide training on best practices for cyber security and physical security standards. This is particularly important for staff who engage in international travel or information sharing, ensuring they are equipped to	**Collaborative Risk Mitigation Plans** Researchers should collaborate with their institution and funder to create risk mitigation plans based on identified areas of concern. These plans should strike a balance between benefits and risks, avoiding hindrances to collaboration, international talent attraction, and sustainable funding. **Specific and Varied Plans** Risk mitigation plans should be highly specific and cover different aspects based on identified risks. They may be integrated into existing research practices, with documented measures shared among project members. These measures should be implemented, monitored, and adjusted as needed. **Familiarity with Controls and Training** All project members should be familiar with the implemented controls.

Recommendations	Government	Research Funders	Research Institutions	Researchers
		Identify and Develop Risk Mitigation Best Practices Review research proposals to identify and establish comprehensive risk mitigation practices. **Broad Circulation of Risk Mitigation Guidance** Disseminate guidance on risk mitigation measures widely within the research community, often in collaboration with government entities.	protect themselves and sensitive information.	Training and onboarding procedures should be established to ensure effective risk management from project initiation through its entire duration.

APPENDIX E. QUESTIONNAIRE FOR RESEARCH INSTITUTIONS AND HIGHER EDUCATION INSTITUTIONS

Research Security Training

1. Does your research organization have a formal research security program?
2. Is a designated individual or department responsible for overseeing the research security program?
3. Does your research organization train relevant personnel on research security threat awareness and identification?
4. How often is research security training conducted for faculty, students, and staff?
5. Does the research security training cover insider threat awareness and mitigation?
6. Are relevant elements of research security integrated into existing training on responsible and ethical conduct of research?
7. In the event of a research security incident, does your research organization provide tailored training to address the incident's specific circumstances?
8. How frequently are research security incidents assessed to determine if additional or updated training is necessary?
9. Does your research organization have a documented process for identifying, reporting, and responding to research security incidents?
10. Should faculty and students complete research security training before starting their research projects?
11. How does your research organization ensure that all personnel are current with the latest research security practices and threats?
12. Are there mechanisms to monitor and evaluate the effectiveness of research security training programs?
13. Does your research organization collaborate with external experts or organizations to enhance research security training?
14. Is research security training customized based on the specific research focus and projects of the personnel?
15. How does your research organization ensure that research security training aligns with the evolving landscape of security threats?

Cybersecurity

1. Does your research institution provide regular cybersecurity awareness training for authorized users of information systems?
2. Does cybersecurity awareness training include recognizing and responding to social engineering threats and cyber breaches?
3. How often is cybersecurity awareness training conducted for authorized users?
4. Does your research institution have mechanisms to limit information system access to authorized users, processes, or devices?
5. Are the types of transactions and functions that authorized users can execute restricted within the information system?

6. How does your research institution verify and control/limit connections to and use of external information systems?
7. What measures are in place to control and safeguard non-public information posted or processed on publicly accessible information systems?
8. How does your research institution identify information system users, processes, and devices?
9. Is authentication or identity verification a prerequisite for access to organizational information systems?
10. How does your research institution monitor, control, and protect organizational communications at the external and key internal boundaries of information systems?
11. Have subnetworks been implemented for publicly accessible system components separated from internal networks?
12. What measures have been implemented to protect scientific data from ransomware and other data integrity attack mechanisms?
13. How does your research institution promptly identify, report, and correct information and information system flaws?
14. Is protection from malicious code in place at appropriate locations within organizational information systems?
15. How does your research institution ensure that malicious code protection mechanisms are updated with new releases?
16. Are periodic scans of the information system and real-time scans of files from external sources performed?
17. How frequently are periodic scans conducted and real-time scans performed?

Foreign Travel Security

1. Does your research organization have established international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, and research purposes?
2. Are the international travel policies also applicable to offers of sponsored travel that may put individuals at risk?
3. How does your research organization maintain a record of covered international travel by faculty and staff?
4. Is there a requirement for faculty and staff to disclose and obtain authorization in advance of international travel?
5. Are security briefings provided to faculty and staff before international travel to ensure awareness of potential risks and safety measures?
6. Does your research organization assist with securing electronic devices (e.g., smartphones, laptops) before international travel?
7. Are there preregistration requirements that faculty and staff must complete before international travel?
8. How does your research organization ensure faculty and staff know the potential security risks of international travel?
9. Are there specific measures to mitigate risks related to sponsored international travel?
10. How does your research organization ensure faculty and staff adhere to the established international travel policies?

Export Control

1. Does your research organization conduct R&D subject to export control restrictions?
2. Are personnel involved in R&D projects subject to export control requirements provided with training on the requirements and processes for reviewing foreign sponsors, collaborators, and partnerships?
3. Is there a specific training program in place to ensure personnel understand compliance with Federal export control requirements?
4. Are personnel trained to identify and handle situations involving restricted entities listed in relevant control lists?
5. How often is the training provided to personnel engaged in export-controlled R&D projects?
6. Is the training customized to address specific scenarios and challenges related to export control compliance?
7. Does the training cover the potential implications of export control violations, including legal and financial consequences?
8. How does your research organization ensure that personnel are up to date with the latest changes in export control regulations?
9. Is there a mechanism to track and verify the export control training completion by relevant personnel?
10. Are there resources available for personnel to seek clarification or guidance on export control compliance matters?