Issue Brief
*June 8, 2026*

# Moving Past a Binary Framework: Openness and Security in International Research Collaboration

*David Biggs*

Photo credit: ImageFlow / Shutterstock.com

*The phrase "as open as possible and as closed as necessary" originated in 2016 as guidance for research data governance under the EU's Horizon 2020 Open Research Data Pilot. Over the following decade, it migrated into national security guidelines, international policy frameworks, and institutional guidance as a governing principle for international research collaboration itself. This migration has had unintended consequences. Applied to collaboration rather than data, the phrase's binary logic implies a zero-sum relationship between openness and security—one in which more of one requires less of the other. This framing alienates researchers who experience security measures as threats to their professional freedom, while simultaneously providing institutional cover for security services to overcorrect toward restriction. This issue brief argues that openness and security are not competing goals but complementary and mutually reinforcing ones, and offers four recommendations for revising policy language to reflect that reality and better support the international research ecosystem it is meant to protect.*

## Introduction

Over the past decade, the phrase "as open as possible and as closed as necessary" has become a common shorthand in discussions of research security.[1] Often paired with calls to "balance openness and security,"[2] it is now embedded in policy documents,[3] institutional guidelines,[4] and international frameworks[5] across the G7, the European Union, and beyond. Horizon Europe itself, which the European Commission describes as "designed to be as open as possible and as closed as necessary," reflects this framing.[6]

While well intentioned, this framing has unintended consequences that go beyond mere linguistic precision. The language used to describe the relationship between openness and security shapes how researchers, institutions, and securi-

ty services understand their respective roles and, crucially, whether they see themselves as partners or adversaries in the same project. When the dominant metaphor is one of finding a balance or a trade-off between two competing goals, the practical effect is often that security is understood as a constraint on collaboration rather than an enabler of it.[7] Researchers interpret calls suggesting that it may be "necessary" to "close" their activities as pressure to limit their international partnerships.[8] Security communities, applying the same binary framing, are inclined to err toward greater restriction when the framing suggests that restriction is the primary or only instrument of protection. Institutions caught between these two orientations struggle to develop coherent, workable policies that serve both while also arguing that the approach fails to allow for the necessity of academic freedom and open science.[9]

A reconsideration of this language is overdue, not as an abstract intellectual exercise, but because the framing actively undermines the goals it is meant to serve. At a moment when international research collaboration is under pressure from multiple directions—geopolitical competition, foreign interference, and the securitization of scientific fields—the last thing the research community needs is policy language that inadvertently reinforces the perception that security and collaboration are in fundamental tension, if not entirely incompatible. Getting this language right is a precondition for getting the implementation right.

***"In the years since its inception, the phrase "as open as possible, as closed as necessary" has been repurposed well beyond its original domain and intent. It now appears in national security guidance and international policy statements to describe not only data governance, but also as a governing principle for the broader conduct of international research collaboration.***

## From Data Governance to Research Collaboration

The phrase "as open as possible, as closed as necessary" was introduced in the context of the European Union's Horizon 2020 Open Research Data (ORD) Pilot, which was initially implemented in the 2014–2016 Work Programmes and formally extended across all thematic areas in the 2017 Work Programme.[10] The ORD Pilot specifies that Data Management Plans must describe how data will be handled, including which datasets will be made open, which will be restricted or closed, and the reasons for limiting access (e.g., security, privacy, or intellectual property).[11] In this original context, the formulation was both practical and appropriate because it addressed a real but distinct problem concerning data access under specific conditions.

Its adoption in research integrity frameworks followed logically. The ALLEA (All European Academies) 2023 revision of the European Code of Conduct for Research Integrity, for example, applies the phrase to proposed data management practices, aligning it with FAIR principles — ensuring that data are Findable, Accessible, Interoperable, and Reusable:

> *"Researchers, research institutions, and organisations ensure that access to data is as open as possible, as closed as neces-*

*sary, and where appropriate in line with the FAIR Principles (Findable, Accessible, Interoperable and Reusable) for data management."*[12]

In the years since its inception, however, the phrase has been repurposed well beyond its original domain and intent. It now appears in national security guidance and international policy statements to describe not only data governance, but also as a governing principle for the broader conduct of international research collaboration. Canada's 2019 National Security Guidelines for Research Partnerships was among the first to extend the principle to the research ecosystem as a whole:

*"To ensure the Canadian research ecosystem is as open as possible and as secure as necessary, the Government of Canada is introducing the National Security Guidelines for Research Partnerships."*[13]

The 2021 G7 Research Compact applied it in the same way, as a guiding principle for effective international collaboration:

*"Openness, reciprocity and cooperation are shared G7 values. We commit to work together to uphold and protect the principles that underpin effective international collaboration that is as open as possible and as secure as necessary."*[14]

The European Council blurred the lines in 2024, including "as open as possible, as closed as necessary" as a principle for Responsible Internationalisation in its Proposal for a Council Recommendation on Enhancing Research Security, and in the final Council Recommendation itself.[15] The principle as written is unclear about whether the phrase applies to research outputs only or to international cooperation itself:

*"continue to promote and encourage international cooperation in research and innovation that is both open and secure, in line with the principle 'as open as possible, as closed as necessary', ensuring that research outputs are findable, accessible, interoperable and reusable (FAIR), with due consideration to applicable restrictions, including security concerns."*[16]

> ***"Framing research partnerships as something that must be either "more open" or "more closed" implies a zero-sum relationship between openness and security. The underlying message—whether intended or not—is that increasing one requires sacrificing the other.***

And in a 2025 public statement, the International Science Council (ISC) took it as a given that the phrase is being applied to the practice of science itself:

*"Science also plays an important role in nations advancing their economic, security, and geostrategic goals. The increasingly used policy mantra of science being "as open as possible and as closed as necessary" must not be extended beyond legitimate need."*[17]

The phrase is now repeated across Europe in frameworks and guidance documents as a "guiding principle" of international collaboration with little to no reflection on its origins or its binary nature. It has been used liberally in recent years in speeches,[18] conference panels,[19] and the media[20] to describe the ideal collaborative research ecosystem, almost always separate from any mention of data, outputs, or the FAIR model

from which it emerged. This conflation—and subsequent shift in application—has blurred an important distinction, one that matters in practice.

## The Limits of a Binary Framework

When applied to data management, the phrase captures a real tension, and the binary quality it implies is not entirely wrong in that context. Digital data is, at its most fundamental level, either shared or not. A datum is released or withheld. A digital file is transmitted or it stays put. Arrangements that appear to complicate this—anonymized datasets, tiered access, aggregated outputs—are still binary at each decision point: specific data elements are shared, or they are not. An analyst who receives confidential income data and then produces and shares an aggregated summary is not sharing the underlying data. They are sharing new data of their own creation, derived from data they received under restricted conditions. The original restriction still holds.

So in the domain of data governance for which it was designed, the phrase's binary logic is not a distortion. It reflects something real about how data access decisions work. The question at each juncture is the same: share this, or don't.

> ***The result is that researchers believe security services and government officials simply do not understand their work or how science operates, while security services and government officials wonder why researchers are so naive about the threats that are all around them.***

Research collaboration, however, does not function in the same way.[21] Framing research partnerships as something that must be either "more open" or "more closed" implies a zero-sum relationship between openness and security. The phrasing itself conjures the image of a door or a window: in order for either to be more closed, it must be less open. The underlying message—whether intended or not—is that increasing one requires sacrificing the other. This is the very definition of a zero-sum game.

This is where the migration of the phrase beyond the realm of data governance becomes genuinely problematic. In the case of a dataset with multiple elements, the more of it that cannot be shared, the less of it that can. A visual of a dial, a door, or a spectrum—with "open" at one end and "closed" at the other—is arguably an accurate representation of a data access decision. The same visual is not an appropriate representation of a complex research collaboration. It is a misrepresentation that carries real consequences.

For researchers, this framing can be consequential and alarming. Scientists' professional identities and career trajectories are built around open exchange—publications, citations, international collaboration, freedom of inquiry, and related practices. If openness is associated with scientific productivity and career advancement, while security is presented as a constraint that limits that openness, then calls to "balance" the two will be interpreted, consistently and predictably, as a demand to limit collaboration and thus damage both scientific careers and science itself.[22] This is not a misreading of the policy intent. It is a natural and rational interpretation of the language as written.

The consequence is increased friction that undermines the very outcomes the policy and messaging should be trying to achieve. Researchers who understand security measures as threats to their professional freedom become skeptical and resistant, or they choose to forgo external collaborations altogether. Institutional administrators caught between security requirements and faculty concerns struggle to implement coherent policies. Trust between the scientific community and the government and security communities erodes—not because either side is acting in bad faith, but because the framing has pre-loaded the conversation with an adversarial structure that need not be there.

From the other side, security services and government officials operating within a "balance" conceptualization face a structurally different but equally problematic dynamic. If openness and security are understood as competing values on the same dial, then any given level of openness can be reframed as a security gap to be closed. Risk-averse institutions—and security organizations are, by their nature, risk-averse[23]—will tend to resolve the balance in the direction of restriction.[24] Not necessarily because they are indifferent to the value of scientific collaboration, but because the framing tells them that more closure means more security, and more security is their mandate. The binary framing, in other words, provides institutional cover for overcorrection in a direction that potentially harms the research ecosystem itself without necessarily making it more secure.

The result is that researchers—trained to share and collaborate openly—believe security services and government officials simply do not understand their work or how science operates,[25] while security services and government officials—whose daily work involves protecting information and absolutely NOT sharing their work products—wonder why researchers are so naive about the threats that are all around them.[26]

> ***"Secure and transparent partnerships that operate under clear, known, and agreed-upon constraints generate confidence among collaborators and their funders, and that confidence supports more robust and open exchange. From this perspective, research security need not be a constraint on collaboration but rather an enabler of it.***

The effect of this on actual research collaboration is visible, even if difficult to quantify precisely. International partnerships have been abandoned or never initiated due to researchers' concerns about security compliance burdens.[27] Foreign students and researchers have faced increased vetting delays, visa restrictions, and reputational risks that deter participation in collaborative programs.[28] Funding agencies have introduced compliance requirements that, while individually defensible, collectively add transaction costs that fall disproportionately on smaller institutions without dedicated research security offices.[29] None of these outcomes is inevitable; but all of them are made more likely by a framing that positions security as a constraint on openness rather than a precondition for it.

In reality, a strong partnership is both open and secure—as the European Council's own Proposal for a Council Recommendation on Enhancing Research Security states directly.[30] The fully transparent nature of real openness creates the

foundation for a secure partnership. And in practice, the more transparency and trust partners share and the more they know about one another's connections and constraints, the more open they can be with one another.[31] Genuine security—built on clear norms, mutual accountability, and transparent processes—can expand the space for collaboration rather than contracting it. The phrase "as open as possible, as closed as necessary" cannot encompass this reality.

## Openness and Security as Complementary Goals

An alternative perspective is already present in policy discussions, though it has not yet displaced the dominant framing: openness and security are not competing objectives, but complementary and mutually reinforcing ones.

This principle was articulated in the G7 Common Values and Principles on Research Security and Research Integrity, which emphasizes directly that "[o]penness and security are not contradictory but complementary and mutually reinforcing."[32] Secure and transparent partnerships that operate under clear, known, and agreed-upon constraints generate confidence among collaborators and their funders, and that confidence supports more robust and open exchange. An institution that can credibly demonstrate that it has effective research security practices—that it knows who its partners are, what guides and constrains them, what is being shared with whom, and under what conditions—is an institution that other serious research institutions would want to work with.[33] Security, in this framing, is not the limiting factor of collaboration; it empowers a more open partnership.

From this perspective, research security need not be a constraint on collaboration but rather an enabler of it. Its purpose is to ensure that international partnerships remain viable, trustworthy, reciprocal, and resilient in the face of evolving risks. The alternative—a research ecosystem that is nominally open but practically vulnerable to foreign interference and coercion, intellectual property theft, and the systematic exploitation of open science principles by actors who do not share its accepted norms—is merely less protected, and over time less sustainable. In the new geopolitical climate, without effective research security measures, the long-term viability of open scientific exchange—one of the primary engines of continued economic growth and public welfare—would be far less certain.

This is a point that deserves to be made with particular force to government officials and policymakers, for whom the zero-sum framing may seem intuitive. Security spending is typically measured against threats prevented, not by the number of secure collaborations enabled.[34] Research programs that function well and produce valuable international partnerships are largely invisible in the metrics of security success.[35] The argument that investment in research security can expand rather than contract the collaborative space requires active and sustained communication—and that communication is made harder, not easier, by language that reinforces a trade-off narrative.

It is also worth noting what the complementarity framing asks of both sides. It asks the research community to accept that not all research is equally targeted, that not all international partners present equivalent risk profiles, and that taking security seriously is an act of professional responsibility rather than political compliance. And it asks the security community to accept that the disruption of research collaboration is itself a national security cost, that overcorrection has potentially severe consequences, and that the goal of research security policy should be a thriving,

resilient international research ecosystem—not the minimization of all international exchange.

These points have been lost in the current discourse.

## Toward More Effective Policy Language

If research security is intended to support, protect, and enable collaboration, then the language used to describe it should reflect that goal. Phrases that imply trade-offs—however unintentionally—can obscure the broader objective of strengthening and improving international research partnerships and alienate the very people whose participation is essential to achieving it.

A more constructive approach would emphasize integration rather than balance: how openness and security can be advanced together through clear norms, transparency, and shared responsibility. Rather than asking which of two values should be prioritized, or how much of one should be sacrificed for the other, the more productive question is: what institutional conditions, partnership frameworks, and shared practices allow both to be pursued simultaneously?

A baker's analogy is apt here. Making a cake does not require a baker to weigh flour against sugar and reduce one to compensate for the other. It requires measuring out the right amount of each, understanding how they interact, and combining them to produce the desired result. The skill is not in the trade-off but in the integration. Effective research security policy works the same way: it asks not how much openness must be sacrificed for security, but what combination of practices, knowledge, norms, and frameworks in a given context produces research collaboration that is genuinely both.

The phrase "as open as possible, as closed as necessary" may retain utility in its original domain of data governance, where it describes a real set of practical decisions about information access. Its use as a governing principle for research collaboration more broadly, however, should be reconsidered—not because the underlying concern is wrong, but because the framing is working against the goal it is meant to serve.

## Recommendations

The following recommendations are offered to policymakers, institutional leaders, and research funders who wish to move toward a more effective framework:

**1. Retire the binary, zero-sum framing from research collaboration policy.** The phrase "as open as possible, as closed as necessary" should be used only in its original context of data governance and data access decisions, where it retains some level of precision and utility. Its application to international research collaboration as a whole should be actively discouraged in future policy documents, guidance frameworks, and public communication. Where the phrase has already been embedded in existing frameworks, a revision note clarifying its proper scope would be appropriate.

**2. Adopt explicit complementarity language.** Policy documents, institutional guidelines, and international frameworks should shift to language that reflects the complementary relationship between openness and security. The G7 Common Values and Principles formulation—that openness and security are not contradictory but complementary and mutually reinforcing—provides a model. "Open and secure" rather than "more open or more closed" should become the governing frame.

**3. Make the argument for security as an enabler explicit and persistent.** Government agencies, funding bodies, and research security offices should invest in communication that frames research security as a needed condition for sustainable collaboration in this era of geopolitical competition and obfuscated intentions, not a constraint on it. This argument should be made directly and specifically to government officials, parliamentary committees, and institutional boards, where the zero-sum framing is most likely to be understood and influence resource allocation and policy decisions.

**4. Evaluate research security policy against collaboration outcomes, not only compliance metrics.** If the goal of research security is a thriving, resilient international research ecosystem, then policy effectiveness should be measured partly by whether secure international partnerships are growing, functioning well, and producing high-quality research with trusted partners—not only by whether compliance requirements are being met. Building these outcome metrics into research security evaluation frameworks would provide a corrective to the tendency toward overcorrection.

## Conclusion

The evolution of the phrase "as open as possible and as closed as necessary" illustrates how policy language can be sretched well beyond its original purpose and, in doing so, create problems it was never designed to address. Originating as practical guidance for data access decisions, the phrase has become a governing metaphor for international research collaboration itself—with consequences for how researchers, institutions, and security services understand their relationship to each other and to the broader project of open science.

Reframing the conversation around the complementarity of openness and security offers a more resilient and more accurate path forward. The goal of research security policy is not to find the right point on a spectrum between openness and closure. It is to build the institutional conditions—transparent norms and constraints, accountable practices, trustworthy partnerships—under which international research collaboration can be both genuinely open and genuinely secure. These are not competing destinations. They are the same destination, reached by the same road.

By emphasizing how these principles work together, and by revising the language used to describe them, policymakers can better support the international research ecosystem they seek to protect—one in which collaboration is not constrained by security, but strengthened and enabled by it.

**Author –**

***David Biggs*** *is a Senior Fellow at ISDP's Stockholm Center for Research and Innovation Security (SCRIS). He is a former U.S. diplomat and Senior Policy Advisor for the U.S. State Department, having served more than 15 years in the foreign and civil service of the United States. His area of expertise is international science and technology (S&T) diplomacy, particularly focusing on research security, global scientific collaboration, and bilateral and multilateral policy development.*



**About ISDP**

*The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.*

www.isdp.eu

## Endnotes

1 Raffaela Kunz, "As Open as Necessary? Research Security, Academic Freedom and the Geopolitics of Science," Verfassungsblog, January 29, 2026.

2 Washington University in St. Louis, "Open Research and Free Dissemination of Ideas and Information, WashU Policy on," December 2016, stating that "the principles of openness must be balanced against the best interests of society."

3 Council of the European Union, "Council Recommendation of 23 May 2024 on Enhancing Research Security," Official Journal of the European Union C/2024/3510, May 30, 2024.

4 University of Freiburg, "Open Science Policy of the University of Freiburg, 2024, stating that research processes and outputs should be "as open as possible and as closed as necessary."

5 Federal Ministry of Education and Research (Germany), "National Action Plan for the European Research Area," 2022, stating that international research cooperation should be "as open as possible and as closed as necessary."

6 European Commission, "Strategic Autonomy and European Economic and Research Security," accessed May 25, 2026, stating that Horizon Europe is designed to be "as open as possible and as closed as necessary."

7 ALLEA, "Research Collaboration and Research Security in a Shifting Geopolitical Landscape," December 18, 2024.

8 "Keep Collaboration Open When Doors Are Closing," *Nature* 585, no. 7826 (2020): 331; Mats Benner et al., "The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security," *Technological Forecasting and Social Change* 201 (2024): 123253.

9 Mats Benner, Sylvia Schwaag Serger, Maria Ljungqvist, and Lucie Vagner, "The Role of Research Funders in Providing Directions for Managing Responsible Internationalization and Research Security," *Technological Forecasting and Social Change* 201 (2024): 123253, arguing that universities and research institutions face difficulties balancing research security with openness, academic freedom, and international collaboration; ALLEA, "Research Collaboration and Research Security in a Shifting Geopolitical Landscape," December 18, 2024.

10 European Commission, "Horizon 2020 Open Research Data Pilot (ORD)," Work Programme context (2016–2017), introducing the principle "as open as possible, as closed as necessary" as the guiding rule for research data governance.

11 European Commission, "Guidelines on FAIR Data Management in Horizon 2020," 2016, implementing the Open Research Data Pilot, which requires beneficiaries to make research data openly available where possible while allowing restrictions for intellectual property, privacy, or security reasons under the principle "as open as possible, as closed as necessary."

12 ALLEA, *The European Code of Conduct for Research Integrity – Revised Edition 2023* (Berlin: ALLEA, June 2023).

13 Government of Canada, *National Security Guidelines for Research Partnerships* (Ottawa: Innovation, Science and Economic Development Canada, 2019).

14 G7, *G7 Research Compact* (2021).

15 European Commission, "Proposal for a Council Recommendation on Enhancing Research Security," COM (2024) 26 final, January 24, 2024; Council of the European Union, "Council Recommendation on Enhancing Research Security," May 23, 2024.

16 Council of the European Union, "Council Recommendation on Enhancing Research Security," recital 5, May 23, 2024, stating that the EU should "continue to promote and encourage international cooperation in research and innovation that is both open and secure, in line with the principle 'as open as possible, as closed as necessary' …"

17 International Science Council, "Protecting Science in Times of Geopolitical Tension," public statement, 2025, stating that "[t]he increasingly used policy mantra of science being 'as open as possible and as closed as necessary' must not be extended beyond legitimate need."

18 See, e.g., European Commission, "Proposal for a Council Recommendation on Enhancing Research Security," COM (2024) 26 final, January 24, 2024; Council of the European Union, "Council Recommendation on Enhancing Research Security," May 23, 2024; CESAER, "Keeping Science Open? Current Challenges in the Day-to-Day Reality of Universities," 2023, describing the shift toward "'as open as possible, as closed as necessary'" as an increasingly common framing in European research-security discourse and policy.

19 CESAER, "Balancing "As Open as Possible" and "As Closed as Necessary", panel discussion at 'Openness and Commercialisation: How the Two Can Go Together,' December 4, 2020.

20 Tom Lindemann and Lisa Häberlein, "Contours of a Research Ethics and Integrity Perspective on Open Science," *Frontiers in Research Metrics and Analytics* 8 (2023), discussing how researchers operationalize the guiding principle "as open as possible, as closed as necessary" in research practice and international collaboration.

21 Peter Smith Ring and Andrew H. Van de Ven, "Developmental Processes of Cooperative Interorganizational Relationships," *Academy of Management Review* 19, no. 1 (1994): 90–118, arguing that collaborations are ongoing relational processes involving negotiation, mutual commitment, informal social expectations, adaptation, and conflict resolution rather than discrete transactions; Elizabeth Zumpe, Peter Piazza, and Katherine Ashton, "Between Transaction and Collaboration: Struggles for Coherence, Responsiveness, and Mutuality in a Fizzled-Out Research-Practice Partnership," *AERA Open* 11 (2025), emphasizing mutuality, responsiveness, and evolving relational dynamics in research partnerships.

22 Michael Polanyi, "The Republic of Science: Its Political and Economic Theory," *Minerva* 1, no. 1 (1962): 54–73, arguing that science operates through decentralized systems of mutual adjustment, reputation, and cooperative competition in which free communication and collaboration are essential to scientific progress; CESAER, "Balancing "As Open as Possible" and "As Closed as Necessary," report on panel discussion at 'Openness and Commercialisation: How the Two Can Go Together,' December 14, 2020, discussing how academic reward systems, publication incentives, and norms of openness shape researchers' responses to restrictions on collaboration and data sharing.

23 Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), explaining that intelligence and security bureaucracies are structurally biased toward caution because the institutional costs of underestimating threats are perceived as much greater than the costs of false alarms; Ben Green and Yiling Chen, "Algorithmic Risk Assessments Can Alter Human Decision-Making Processes in High-Stakes Government Contexts," 2020, finding that introducing security-oriented risk assessments made government decision-makers "more risk-averse" in public-sector policy contexts.

24 Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (New York: Copernicus Books, 2003), emphasizing that security institutions operate through precautionary trade-offs and tend toward conservative responses under uncertainty.

25 John J. Hamre, "Science and Security at Risk," *Issues in Science and Technology* 18, no. 4 (Summer 2002), stating that "Scientists, in turn, believe that security professionals do not understand the nature of science and thus pursue procedures designed to demonstrate compliance with rules more than securing secrets."

26 John J. Hamre, "Science and Security at Risk," *Issues in Science and Technology* 18, no. 4 (Summer 2002), stating that "[s]ecurity professionals feel that scientists either do not understand or fail to appreciate the threats and thus cannot be trusted to protect U.S. secrets without explicit and detailed rules and regulations."

27 Jack Grove, "Research Security Checks 'Cost Universities £11 Million a Year'," *Times Higher Education*, March 8, 2023, reporting that increased due-diligence and compliance requirements around international research partnerships were "overwhelming" and "demoralising" staff, and noting that some UK-China research partnerships "have now closed" under the growing burden of research-security regulation.

28 Hannah Devlin, "Foreign Office Vetting Deterring Top Scientists from UK, Royal Society Warns," *Guardian*, November 7, 2022, reporting that security-vetting delays and restrictions were discouraging international researchers from taking up collaborative scientific positions in the UK; "US Collaboration Affected by Security

Checks," *CORDIS* (European Commission), August 26, 2002, describing how visa security checks delayed or postponed international scientific workshops and collaborations involving foreign researchers.

29 Council on Governmental Relations (COGR), "Research Security and the Cost of Compliance—Phase I Report: Disclosure Requirements, 2022, finding that expanding federal research-security compliance requirements impose significant administrative and financial burdens, especially on smaller institutions lacking developed compliance infrastructure and dedicated personnel; National Academies of Sciences, Engineering, and Medicine, *Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop* (Washington, DC: National Academies Press, 2025), discussing how research-security compliance requirements create disproportionate burdens for smaller institutions lacking dedicated research-security personnel and infrastructure.

30 European Commission, "Proposal for a Council Recommendation on Enhancing Research Security," COM (2024) 26 final, January 24, 2024, emphasizing the objective of "ensuring that international cooperation in research, innovation and higher education remains both open and secure."

31 Canadian Institute for Environmental Law and Policy, *Making the Most of Partnerships* (Toronto: CIELAP), "...it is vital that collaborators be well informed about what others are doing if they are going to trust one another and work efficiently together."

32 G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE), *G7 Common Values and Principles on Research Security and Research Integrity* (June 2022).

33 Bram Klievink, Haiko van der Voort, and Wijnand Veeneman, "Creating Value Through Data Collaboratives: Balancing Innovation and Control," *Information Polity* 23, no. 4 (2018), arguing that "Trust is said to facilitate interaction among actors by lowering transaction costs."; Also see Peter S. Ring and Andrew H. Van de Ven, "Developmental Processes of Cooperative Interorganizational Relationships," *Academy of Management Review* 19, no. 1 (1994): 90–118, .

34 Shahar Perets, "Rationalize Security Spend: Exposure Management & Security Validation," Security Magazine, October 30, 2023, noting that in security governance "it can be difficult to quantify a breach that didn't happen."

35 Jody L. Jacobs, Julie M. Haney, and Susanne M. Furman, "Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study," presented at the 10th International Conference on HCI in Business, Government and Organizations (HCIBGO 2023), stating: "We discovered that organizations do indeed place emphasis on compliance metrics and are challenged in determining other ways to gauge success."