NOBRIS

*Technical Compliance. Strategic Awareness.*

# Research Security Is Not Export Control

March 2026

Nobris Industries Corporation

## What Research Security Actually Does

Research security happens before the work begins. Before the collaboration is signed. Before the first experiment runs. It asks a set of questions that most organizations only think about after something goes wrong: [1]

Have we submitted all required disclosures to conduct this work? Are we partnering with individuals or organizations that appear on a government watch list? Does our institution understand and accept the reputational and funding risk of this collaboration? [3, 4]

Research security also asks whether the proposed partner has been forthcoming in their own disclosures. What does their collaborative network look like? Who else are they working with, and does that context change the picture?

The core question is: do we know our partners well enough to be both technically compliant and strategically aware? [2]

## Where Export Control Fits

Export control looks at defined work and asks: am I prevented from sharing this technology or data with this foreign entity? It is an intrinsic part of the research security function, but the two sit at different ends of the timeline. [5, 6]

Research security casts a wide net while organizations are still scoping a collaboration. It gives decision-makers the context to say we accept this risk or we don't. Export control looks at the output and asks whether the institution lived up to its obligations.

They are complementary. But treating them as interchangeable creates gaps. An institution can be fully export-control compliant and still walk into a collaboration that damages its reputation, threatens its funding, or ends up in a congressional report. [7, 14]

## The Broader Threat Landscape

The research security conversation often defaults to military concerns, and for good reason. Several countries operate under policies that blur or erase the line between civilian research and defense applications. China's civil-military fusion strategy is the most cited example, but it is not the only one. Other nations direct academic research toward state industrial objectives in ways that do not map neatly onto Western distinctions between civilian and military institutions. [8, 15]

But the risk is not limited to military modernization. Research security also addresses economic security. When a foreign government targets critical and emerging technologies through academic collaboration, the concern is not only that the research could support weapons development. It is also that it could accelerate a competitor's industrial capacity in areas like advanced semiconductors, artificial intelligence, quantum computing, or biotechnology. The economic consequences of unchecked technology transfer can be as significant as the national security ones. [9]

This is why research security cannot rely on entity lists alone. A university that does not appear on any sanctions or export control list may still be embedded in a foreign government's defense-industrial ecosystem. The institution's role in that ecosystem is exactly the kind of context that research security is designed to surface. [10, 11]

## The Co-Authorship Problem

Research security matters in part because outside observers rarely understand the complexity behind a published scientific paper. When a security firm, a congressional staffer, or a journalist sees a publication co-authored by a US researcher and someone affiliated with a foreign institution tied to a country's defense or industrial policy apparatus, they draw a straight line. The assumption is that these researchers sat in the same lab, shared the same data, and worked toward the same goal. [12]

The reality is almost never that simple. There are many ways a US researcher can end up named on a paper alongside someone from a flagged institution without any wrongdoing having occurred.

**The researcher left.** A foreign collaborator was in the US on a visa, contributed to early-stage work, and returned home before the paper was finalized. Their name stays on the paper because they contributed. Their current affiliation shows the foreign institution. The work happened entirely on US soil.

**The institution changed.** A co-author was affiliated with a civilian university at the time of the research. That university was later designated under a watch list. The paper now shows an affiliation with a restricted entity, but the collaboration predates the designation.

**The co-authors never actually worked together.** Large multi-institutional projects can produce papers with dozens of named authors. A researcher at one site may have no direct interaction with a researcher at another. Authorship conventions in some fields include anyone who contributed to the broader project, not just the specific analysis.

**A third party facilitated the connection.** An equipment manufacturer, a shared facility, or a national lab ran an experiment. Multiple groups submitted samples or data. The resulting paper lists all contributors, but the groups may never have communicated directly or shared anything beyond the published results.

**Fundamental research was involved.** The work falls under the fundamental research exclusion and was intended for open publication from the start. No access controls were required. No export-controlled information was exchanged. The collaboration was permissible under every applicable regulation. But the partner institution contributes to military-relevant research in other programs, or works on critical and emerging technologies that a foreign government has prioritized. The US institution was technically compliant but had no visibility into the broader strategic context of its partner's work. [5, 7]

These scenarios do not account for every case, and context matters. But they illustrate why a publication record alone is not evidence of a security failure. Without the context that research security provides, every foreign co-authorship looks the same from the outside. [4]

## Why This Matters

Research security is imperfect. It does impact science. It creates a structure that asks researchers conducting fundamental research, and their parent organizations, to confront difficult questions: is the value of this science worth the risk to future funding if the collaboration ends up in a report that says the institution contributed to another country's military capabilities, or gave a strategic competitor an advantage in a critical technology area? [13, 4]

The consequence is that not every collaboration will be approved. The science will not always win out. But the benefit is that when the institution does approve a collaboration, it can explain why. And when it declines one, it can explain that too. Future funding stays on the table because the institution demonstrated judgment, not just compliance.

That is what research security gives you that export control alone cannot.

## References


1. National Science and Technology Council. Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development. January 2022.
2. White House Office of Science and Technology Policy. Guidelines for Research Security Programs at Covered Institutions. July 9, 2024.
3. Strouse, G. F., Wood, T. R., Saundry, C. M., Bennett, P. A., & Bedner, M. Safeguarding International Science: Research Security Framework. NIST IR 8484. National Institute of Standards and Technology, August 2023. DOI: 10.6028/NIST.IR.8484.
4. U.S. Government Accountability Office. Research Security: Agencies Should Assess Safeguards Against Discrimination. GAO-26-107544. January 2026.
5. 15 C.F.R. § 734.8, Fundamental Research (Export Administration Regulations).
6. Bureau of Industry and Security. "What Is a Deemed Export?" https://www.bis.gov/learn-support/deemed-exports/what-deemed-export
7. 22 C.F.R. § 120.34, Public Domain (International Traffic in Arms Regulations). Note: formerly numbered § 120.11 prior to ITAR restructuring.
8. U.S. Department of Defense. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025. December 2025.
9. National Science and Technology Council. Critical and Emerging Technologies List Update. February 2024.
10. U.S. Government Accountability Office. Research Security: Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats. GAO-24-106227. January 2024.
11. 15 C.F.R. Part 744, Control Policy: End-User and End-Use Based (Export Administration Regulations). See § 744.16 for Entity List definition.
12. Gallo, M. E. Small Business Research Programs: Selected Issues for Reauthorization. CRS Report R48629. Congressional Research Service, December 15, 2025.
13. The White House. Presidential Memorandum on United States Government-Supported Research and Development National Security Policy (NSPM-33). January 14, 2021.
14. U.S. Government Accountability Office. Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities. GAO-22-105727. May 2022.
15. Imbrie, A. & Fedasiuk, R. "Untangling the Web: Why the U.S. Needs Allies to Defend Against Chinese Technology Transfer." Brookings, April 2020.