



Your Research. Our Mission.



RESEARCH SECURITY LANDSCAPE REPORT

Research Security in U.S. Federally Funded Science: Evidence, Exposure, and a Risk-Calibrated Path Forward

From exposure to action: A 10-year analysis of research security risk in U.S. federally funded science

Dr. Xueying (Shirley) Han, Digital Science

Contents

Foreword	1
Executive Summary	3
What Is Research Security, and Why Now	5
The Aim of This Report	7
Evidence: What the Data Show	8
A Risk-Calibrated Framework	13
Conclusion: Toward Proportionate Vigilance	16
Appendix	17



Foreword

When the U.S. government announced its ‘pivot to Asia’ in 2011, the political signal was clear: engagement with China and the Asia-Pacific was a strategic priority. Universities, funding agencies, and companies heard and responded accordingly. Chinese student enrollment at U.S. institutions nearly tripled over the following decade. NIH and China’s National Natural Science Foundation signed cooperation agreements and launched joint funding calls. Cross-border research co-authorship grew at 20% annually through 2017. The architecture of deep interdependence was built quickly and, in many places, without adequate attention to the asymmetry at its foundation: the engagement was largely genuine on one side and strategically instrumental on the other.

Those inside the intelligence community who understood that asymmetry were raising concerns well before the public policy debate caught up. By 2015, FBI counterintelligence officers were conducting quiet briefings at major research universities, warning that China’s Thousand Talents Program — launched in 2008 — was not simply a talent development initiative but a structured mechanism for acquiring intellectual property and scientific knowledge and returning it to China. This awareness, however, was also largely confined to classified channels, siloed from the researchers, administrators, and policymakers who were building those collaborative relationships in good faith. It was not until FBI Director Christopher Wray’s public speech in July 2018 that the warning began to reach the level of public policy discourse — and not until the JASON scientific advisory panel’s landmark “Fundamental Research Security” report in December 2019 that the field had anything resembling a rigorous conceptual framework.

What has emerged from that reckoning is, however, not a settled consensus but a polarized debate. One camp argued that the threat was systemic and required dramatic restriction of international research collaboration. The other argued that such restrictions would do more damage to allied scientific capacity than any adversarial acquisition program. Both camps were operating largely on anecdote, case study, and ideological instinct. Neither had sufficient data.

The report you are reading begins to change that. Its findings are instructive and, in some cases, surprising. Research security exposure to entity-list affiliations in U.S. federally funded science has declined for six consecutive years — a 29% reduction from its 2018–2019 peak — while the volume of international collaboration has remained largely stable. Researchers are not withdrawing from the world; they are making more careful choices about with whom they work. And yet the same data shows a sharp spike in flagged researcher activity in 2024, demonstrating that this progress is fragile. Perhaps most consequentially, nearly half of the researchers identified as security risks held U.S. affiliations for 24 months or less — a population of short-term visiting scholars who fall almost entirely outside the current disclosure framework.

Treating research security as either an emergency requiring blanket restriction, or a compliance process to be administered and filed, produces the same outcome: institutions that are simultaneously over-burdened and under-protected. The binary is not just analytically wrong. It is operationally naive. The right frame is neither blanket restriction nor simple compliance. It is contextual knowledge and intelligence: precise, longitudinal understanding of what is actually happening.

The data in this report starts us down that road. It provides a rigorous baseline against which future years can be measured, trends are identified early, and policy responses are calibrated to actual risk. Used well, these and future findings should help institutions ask better questions: not “are we compliant?” but “how do these collaborations affect us, where is our actual exposure, and are we addressing it in ways that protect our research mission rather than undermine it?” Rather than offering researchers just two inadequate options — restriction without nuance or openness without awareness — the more productive frame is a third: equip researchers with the knowledge and data they need to make genuinely informed decisions about their collaborations.

The evidence in these pages demonstrates that openness and security can and do co-occur — when the framework is clear enough and provides enough information to distinguish a genuine risk from a false alarm. Read it carefully. Use it critically. And come back next year to see what has changed.

I am grateful to the Digital Science team for the methodological rigor and intellectual honesty they brought to this work, and I look forward to seeing more of the picture as it continues to evolve and as the team works to pull the veil back more and more.

David Biggs

Senior Fellow, Institute for Security and Development Policy (ISDP), Stockholm Center for Research and Innovation Security (SCRIS)

Visiting Research Fellow, UNU-CRIS

Former Team Lead, Office of Science and Technology Cooperation, U.S. Department of State



Executive Summary

U.S. federal research security policies have matured rapidly since 2021. Tightened federal guidance and requirements on biographical sketches and current and pending (other) support are now complemented by new guidance and policy governing collaborations and affiliations with foreign institutions that appear on restricted entity lists. The shift from a trust-based, honor-system model to one of verification and enforcement has left both research institutions and federal agencies in a gray zone, balancing scientific openness and collaboration against the need to protect federally funded intellectual property, scientific knowledge, and research infrastructure from U.S. adversaries. A primary reason for that uncertainty is a lack of understanding of how big the problem actually is. This report addresses that directly, providing a rigorous, ecosystem-wide assessment of the research security exposure facing U.S. federally funded research.

This report draws on publication, funding, and affiliation data from the Dimensions database for 2016–2025, and proposes an operational, risk-calibrated framework for how research institutions and U.S. federal agencies can act on the findings. The key takeaways from this assessment of the U.S. research security landscape are:

Visiting scholars and short-term appointees are a policy blind spot.

Approximately half of flagged researchers had U.S. affiliations lasting 24 months or less, as determined by their publication activity. This pattern is more consistent with visiting appointments than with continuing faculty, and one that current disclosure forms are not built to catch and that research security policies do not address.



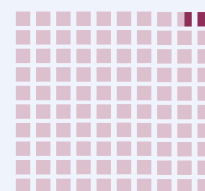
48.2%

A modest number of flagged researchers are receiving federally funded dollars shortly after an entity-list affiliation. At least \$6.8 billion in federal funding (1.1% of all U.S. federal research funding, 2016–2025) has gone to 1,687 U.S. researchers after having an entity-list affiliation. Over 35% were funded within 12 months of their last entity-list tie, and three-quarters within 36 months.



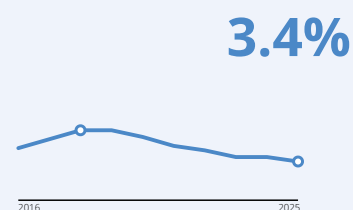
\$6.8B

The at-risk population is identifiable and narrow. Since 2016, 29,423 of the 1,943,748 U.S.-affiliated researchers on U.S. federally funded publications (1.5%) held a U.S. and an entity-list affiliation in the same calendar year, with roughly 5,194 researchers active in any given year. This risk is geographically concentrated with 92.4% of flagged researchers' entity-list ties tracing to organizations in China.

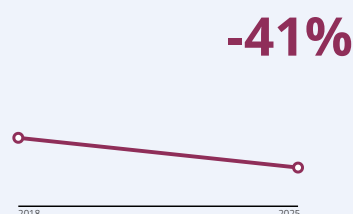


1.5%

Exposure is persistent, but shows signs of declining. Among the ~3 million U.S. federally funded publications produced between 2016 and 2025, the share carrying an entity-list-affiliated researcher peaked at 4.8% in 2018–19 and has fallen to 3.4% in 2025, a 29% relative decline. That six-year decline reversed briefly in 2024 with a single-year spike in flagged-researcher activity (Section 3.6), a reminder that this trend needs continuous monitoring rather than periodic review.



International collaboration risk is falling faster than exposure overall. Among federally funded publications with at least one U.S. and one non-U.S. co-author, the share involving an entity-list-affiliated collaborator peaked at 13.3% in 2018 and has fallen to 7.9% in 2025 (a 41% decline) even as the total volume of that international collaboration has stayed essentially stable, ranging between roughly 78,000 and 94,000 papers a year.



These findings suggest that there doesn't have to be a choice between scientific openness and protecting federally funded research and knowledge. Blanket restrictions on international collaboration do not take into account a landscape where federally funded research appears to be naturally shifting toward less risky international collaborations, and the overall exposure risk appears small (roughly one U.S. researcher in 70). This suggests that there is a behavioral shift with researchers choosing to collaborate more with lower-risk international partners rather than withdrawing from international collaboration altogether, evidence that openness and security can co-occur. These findings argue for a more calibrated response rather than a uniform, one-size-fits-all posture.

Taken together, we propose a risk-calibrated framework for research security. Every researcher applying for federal funds is verified against the same baseline of research security checks. To better balance openness and collaboration against protection, we recommend a risk-calibrated cooling-off period, with the strictest consequences applied to research in critical and key technology areas. The length of that cooling-off period should scale based on an institution's or agency's declared risk tolerance, and it is up to individual institutions to decide what safeguards, if any, they want in place for visiting scholars and short-term appointees, a population current federal policy does not yet address.

These findings suggest that there doesn't have to be a choice between scientific openness and protecting federally funded research and knowledge.

1. What Is Research Security, and Why Now

For most of the past 80 years, U.S. scientific leadership has rested on the idea that openness (i.e., the free movement of people, data, and ideas across borders) produces more innovation, economic growth, and societal good than it puts at risk. This view has enabled a proliferation of scientific and technological advances, achieved through international collaboration and partnership. However, the same openness that made the United States a global scientific powerhouse is now a channel that foreign state-sponsored actors can exploit to shortcut years of foundational and translational research and development (R&D), also known as ‘scientific leapfrogging.’

The [National Science and Technology Council](#) defines research security as the protection of the U.S. R&D enterprise against misappropriation, undue foreign interference, and violations of research integrity. In practice, this means ensuring that when U.S. federal dollars fund a breakthrough, the resulting intellectual capital is disclosed honestly to funding agencies and institutions, tracked accurately, and protected from direct transfer to the military or intelligence programs of U.S. adversaries.

U.S. research security policy today operates on a two-tiered framework, with cross-agency requirements establishing a common baseline (Table 1) and individual departments and agencies layering on additional, often more stringent, requirements (Table 2).

Table 1. Cross-agency research security policy drivers and summary of requirements for each.

Policy Driver	Summary of Requirements
<u>NSPM-33</u> (Jan. 2021; NSTC guidance Jan. 2022 and OSTP memo to federal agencies July 2024)	Standardized disclosure across NSF, NIH, and other agencies; complete disclosure of all appointments, including honorary or voluntary roles; an expanded Current & Pending (Other) Support definition covering all domestic and foreign support, in-kind contributions over \$5,000, and externally paid (“embedded”) personnel; mandatory persistent digital identifiers (e.g., ORCID); and a formal research security program requirement for institutions receiving more than \$50M/year in federal science and engineering funding, with full compliance expected by the end of 2026.
<u>CHIPS and Science Act of 2022</u> (Public Law 117-167)	Requires federal grant applicants to certify they are not participating in a Malign Foreign Talent Recruitment Program (MFTRP).
<u>False Claims Act enforcement</u> (31 U.S.C. §§3729–3733)	A federal law imposing civil liability on institutions that knowingly submit false claims for government funds. When a research institution applies for federal funding, it certifies that all required disclosures, including a researcher’s foreign affiliations and support, are complete and accurate. If that certification is false because the institution failed to verify what a researcher did or didn’t disclose, the institution, not just the researcher, can be held liable, with the government required to show only ‘reckless disregard’ or ‘deliberate ignorance,’ not intent.

Table 2. Agency-specific implementation.

Policy Driver	Summary of Requirements
Wolf Amendment (Section 1340, P.L. 112-10, 2011; renewed annually)	Bars NASA and the White House Office of Science and Technology Policy (OSTP) from using federal funds for bilateral programs, contracts, or coordination with China or any Chinese-owned company without specific congressional authorization and FBI certification that no risk of technology transfer exists. It is one of the earliest China-specific research restrictions in federal law and still in force today.
<u>Department of Defense Section 1286 funding prohibition</u> (FY2025 list update, released June 2026; prohibition effective FY2026)	The Department of Defense is now prohibited from obligating or expending any funds for fundamental research involving collaboration with an entity on the current NDAA §1286 list. The funding bar applies to grants, contracts, and other assistance to institutions of higher education; extends to all employees of listed institutions; and separately requires researchers to disclose any affiliation with a listed entity or foreign talent recruitment program.
NSF Dear Colleague Letter on foreign collaborations (NSF 26-022, July 2026)	Starting in FY2027, NSF funds are prohibited from supporting collaboration with organizations on U.S. restricted-party lists. Senior/key personnel will be barred from holding an appointment with, receiving support from, or collaborating with a restricted entity for the duration of an NSF award, certified at proposal submission.

The cumulative effect of these drivers is a fundamental shift in who bears the burden of proof. An institution can no longer treat a researcher’s self-disclosure form as the end of its due diligence. Under the False Claims Act’s reckless-disregard standard, institutions are expected to have verified what they should have known, not merely to have accepted what a researcher chose to disclose. That standard exists because some Malign Foreign Talent Recruitment Programs contractually prohibit participants from disclosing their participation.

2. The Aim of This Report

Despite the fast-changing federal research security policy landscape described above, there is no comprehensive assessment of how widespread entity-list-linked research activity is across U.S. federally funded research. Compliance officers, university leadership, and federal program managers have been interpreting policy and deciding how much scrutiny is enough, largely without understanding the landscape they are operating in.

The risk in reacting without fully understanding the landscape is two-fold. It is easy to overreact: imposing blanket restrictions that hinder low-risk international collaboration, drive a brain drain by deterring talent from coming to the United States and pushing talent already here to leave, and impose compliance costs disproportionate to the actual exposure. It is equally easy to under-protect: treating research security as a low priority compliance check and risking a future in which taxpayer-funded knowledge and research breakthroughs flow to foreign adversaries, potentially leaving the United States at a long-term strategic and economic disadvantage.

This report establishes a research security baseline for the United States using publication, funding, and affiliation data from the Dimensions database (Section 3); translates the findings into a risk-calibrated framework intended to help institutions and agencies find the balancing point between openness and protection that matches their own risk tolerance (Section 4); and closes with a shared responsibility model for putting that framework into practice (Section 5).

Compliance officers, university leadership, and federal program managers have been interpreting policy and deciding how much scrutiny is enough, largely without understanding the landscape they are operating in.



3. Evidence: What the Data Show

Research security exposure can arise through more than one pathway, and each carries a different level of visibility to standard disclosure and compliance checks. Sections 3.1 through 3.4 examine four such pathways: (3.1) the overall share of federally funded research that has any entity-list ties; (3.2) researchers who personally hold a U.S. and an entity-list affiliation at the same time; (3.3) U.S. researchers who collaborate with entity-list-affiliated researchers; and (3.4) how quickly researchers receive federal funding after their entity-list affiliation ends, when relationships and channels of communication from that tie are most likely still active. Section 3.5 then identifies a research security gap, transient researchers, that current guidance and policy do not yet address, and that may pose an exposure risk largely invisible to the measures above.

3M+

federally
acknowledged
publications
since 2016

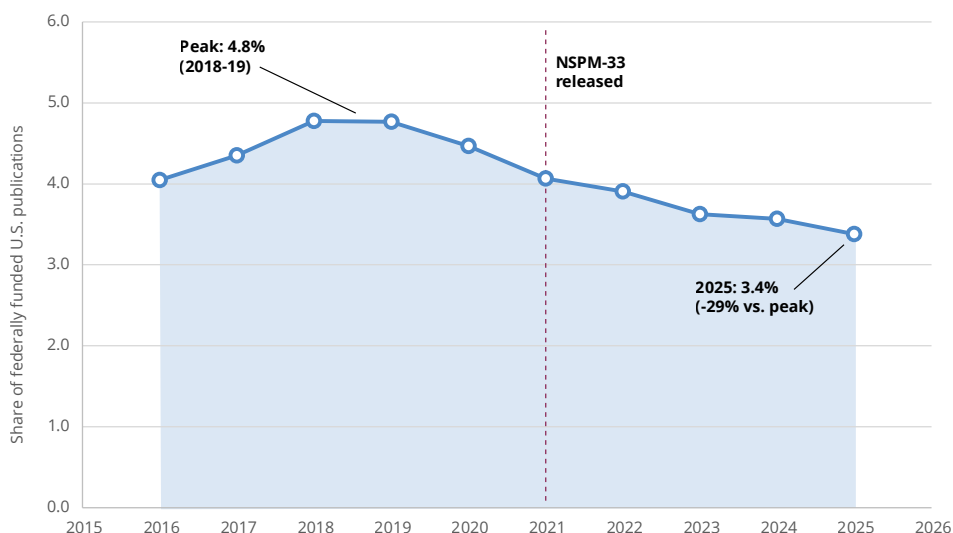
305K

average
publications
per year

3.1 Modest Exposure Across Federally Funded Research

The overall research security exposure of federally funded research is relatively modest and has been decreasing. Since 2016, U.S. researchers have produced more than 3 million publications acknowledging federal support with an average of approximately 305,000 publications per year (Figure 1). Of U.S. federally funded publications, the share of publications that contained an entity-list affiliation peaked at 4.8% in 2018–19, a few years before NSPM-33's release, and has declined for six consecutive years to 3.4% in 2025, a 29% reduction in relative exposure from the peak.

Figure 1. Share of federally funded U.S. publications with an entity-list affiliation, 2016–2025.



3.2 Direct Exposure: A Small, Identifiable Population

Research security exposure is concentrated in a small population of researchers. Of the 1,943,748 U.S.-affiliated researchers who appeared as authors on the more than 3 million federally funded

publications produced between 2016 and 2025, 29,423 (1.5%) held a U.S. and an entity-list affiliation in the same calendar year (referred to as ‘flagged researchers’ hereafter). There are, on average, 5,194 flagged researchers who are active in a given year (Figure 2).

Two forms of research security exposure. A flagged researcher represents the most direct form of exposure: someone who worked on federally funded research while simultaneously holding an entity-list affiliation, making some degree of knowledge transfer likely. Section 3.3 addresses a second, less direct form: collaborating with a researcher who holds an entity-list affiliation.

The exposure is heavily concentrated in one country: 92.4% of flagged researchers’ entity-list ties trace to China, which is higher than China’s 84.6% share of all entity-list organizations (Figure 3). Entity-list ties with Russia (3.8%) and Iran (3.5%) are secondary but notable. Iran’s share of flagged researchers is disproportionately high relative to its 0.7% share of entity-list organizations, pointing to concentrated risk within a small number of institutions rather than a broad national footprint.

29,423
unique flagged
researchers
since 2016

~5,194
active in a given year

1.5%
of the U.S.-affiliated
researcher
population

Figure 2. Flagged researchers by year and share of the U.S.-affiliated researcher population, 2016–2025.

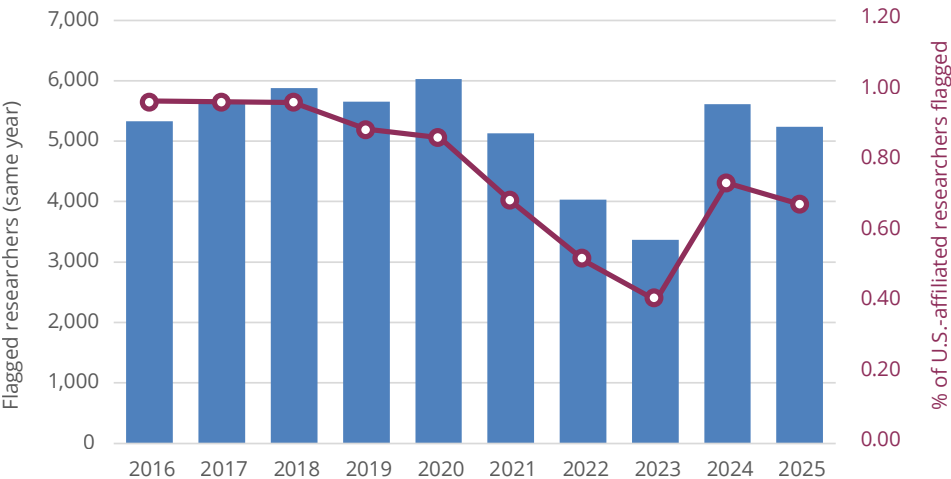
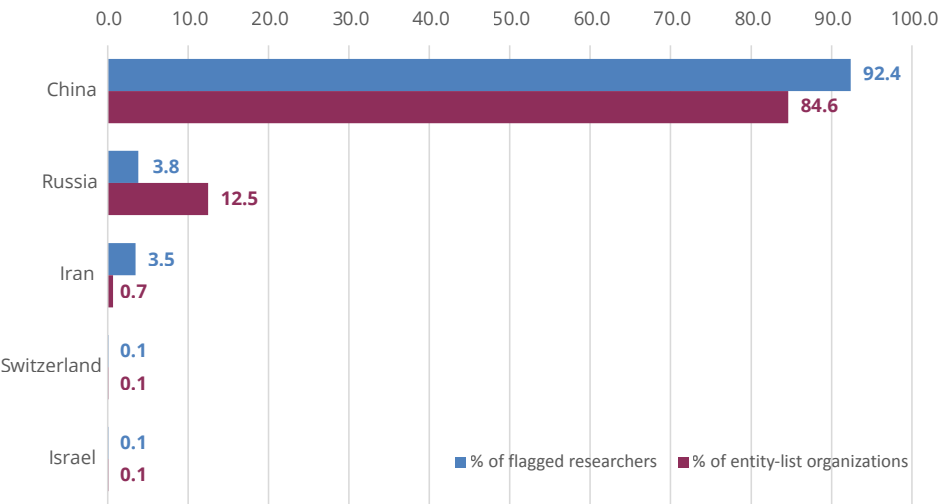


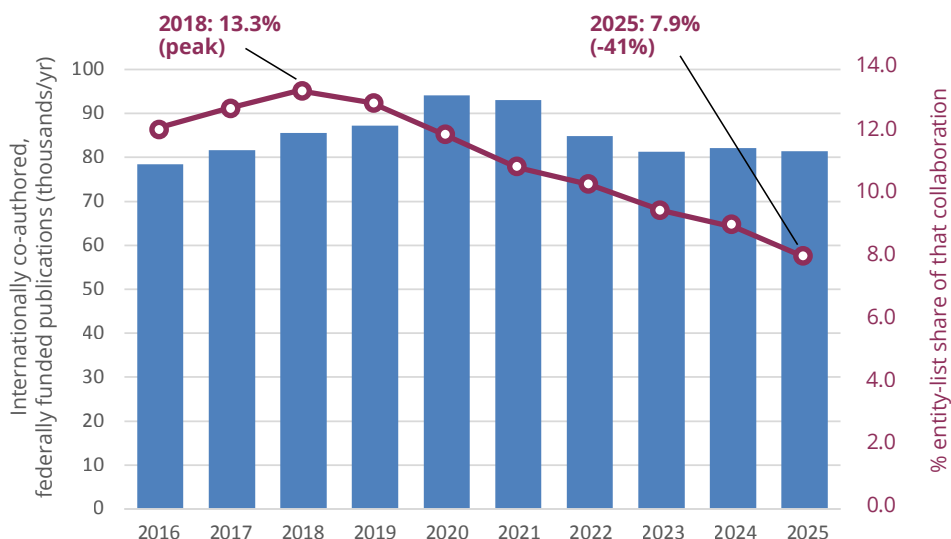
Figure 3. Country concentration of entity-list risk: share of flagged researchers vs. share of entity-list organizations.



3.3 International Collaboration Is Getting Safer

Among federally funded publications with at least one U.S.-affiliated author and one non-U.S. co-author, the share involving an entity-list-affiliated collaborator peaked at 13.3% in 2018 and has fallen every year since, to 7.9% in 2025, a 41% decline (Figure 4). This decline has come even as the underlying volume of international collaboration has stayed relatively stable, ranging between roughly 78,000 and 94,000 papers a year. This suggests that there is a behavioral shift with researchers choosing to collaborate more with lower-risk international partners rather than withdrawing from international collaboration altogether, evidence that openness and security can co-occur.

Figure 4. Total internationally co-authored, federally funded publications (left axis) vs. the entity-list share of that collaboration (right axis).



3.4 Federal Funding Exposure: Few Researchers, Sizable Dollars, Fast Re-Entry

Since 2016, 1,687 U.S.-affiliated researchers have received a minimum of ~\$6.8 billion in U.S. federal funding after having an entity-list affiliation, equal to 1.1% of all U.S. federal research funding over the period. How soon a researcher receives federal funding after an entity-list affiliation is the more concerning signal. Over 35% of this group received a federal award within 12 months of their last entity-list affiliation, and three-quarters did so within 36 months (Figure 5).

That such a large share of researchers received federal funding within 12 months of having an entity-list affiliation suggests that federal agencies (and research institutions) may not have had systematic mechanisms in place to review and identify research security risk at the time of award. In addition, some of this activity likely predates today's research security policies, given how recently certain policies have been made. It does highlight, however, the kind of pattern institutions and funding agencies should now check against.

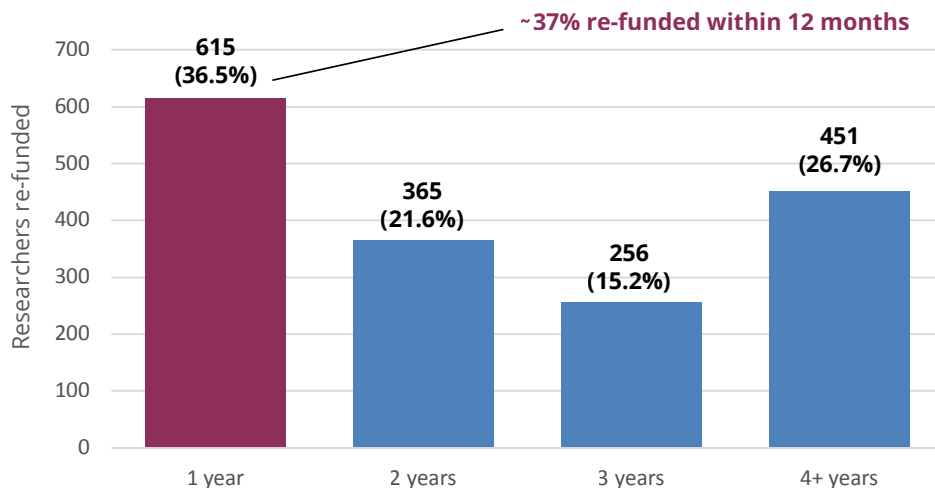
\$6.8B+

federal funding after an entity-list affiliation (1.1% of all federal funding)

1,687

researchers funded by federal agencies after entity-list affiliation

Figure 5. Years between a researcher's last entity-list affiliation and their first subsequent U.S. federal grant.

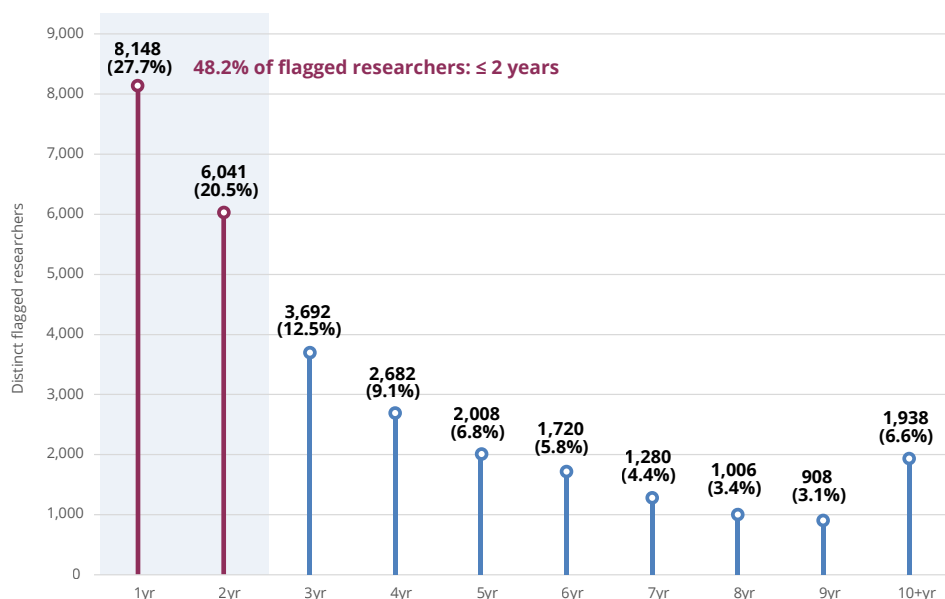


3.5 A Policy Gap: Transient Researchers

Approximately half (48.2%) of flagged researchers held a U.S. affiliation for 24 months or less (Figure 6). This is a pattern more consistent with visiting scholars and short-term appointees than with tenured or tenure-track faculty. The current disclosure landscape, including the Common Forms, is built around the biographical and funding history of continuing faculty who submit federal proposals under their names. It has little natural mechanism for surfacing risk carried by a visiting researcher who is embedded in a lab, with access to data, equipment, seminars, personnel, and ideas, but never personally needs to file a federal disclosure form.

This blind spot presents a genuine risk because it is difficult to detect until it has already taken place. While a visiting scholar or short-term appointee is physically embedded in a U.S. research institution, the publications produced during that window will likely list the U.S. institution as their affiliation but they may not list the entity-list organization from their home country. A researcher collaborating with that visitor in real time would be, correctly, disclosing a U.S.-based colleague; there is no active foreign affiliation to catch at that moment. The entity-list tie only becomes visible in the data retrospectively, once a researcher's full affiliation history is reconstructed across institutions and years. This means the research security risk of knowledge transfer occurs and is likely not detectable during a standard affiliation-based check.

Figure 6. Distinct flagged researchers by total length of U.S. affiliation on funded publications, 2016–2025.



Policy gap: disclosure forms are built around long-term faculty; the population carrying nearly half of all entity-list exposure is short-term visitors who fall largely outside that frame.

3.6 Key Takeaways

- **First**, U.S. research security risks appear to be decreasing: relative exposure has declined for six straight years. The drop in collaboration-level risk suggests an active shift toward safer international collaborators.
- **Second**, progress is fragile: a single-year spike in flagged researcher activity in 2024, following several years of decline, shows that research security exposure can increase sharply and without warning. This highlights the need for continuous data monitoring and researcher education on the national security implications of their research and collaboration choices, rather than periodic compliance reviews alone.
- **Third**, a sizable amount of federal funding is reaching a modest number of researchers quickly after an entity-list affiliation: much of what has been observed likely predates the current wave of research security policy, but it provides a baseline for tracking how this may change going forward. Whether the amount of federal funding reaching researchers immediately after an entity-list affiliation lessens over time as these policies are implemented and mature will be worth watching over the next several years.
- **Fourth**, transient researchers pose a potential research security policy gap: visiting scholars and short-term appointees with entity-list home affiliations may be invisible on federal disclosure forms, since their affiliation of record during a visit is the U.S. institution, not their home tie. Current federal policies do not have specific guidance for this group, which may warrant additional consideration by research institutions and federal agencies on how best to mitigate this risk.

See the Appendix for full methodology and data limitations.

4. A Risk-Calibrated Framework

A framework for federal funders and research institutions to translate the evidence in Section 3 into a proportionate, defensible screening and response process, calibrated to each organization’s risk tolerance rather than applied uniformly.

The proposed framework rests on two premises: not all research carries equal national security weight, and not all institutions or agencies have the same risk tolerance. Together, they translate into four recommended steps: Classify, Screen, Assess, and Act. Sections 4.1 through 4.4 map directly onto these four steps. Sections 4.5 and 4.6 then extend the framework beyond the individual researcher and the four steps themselves.

CLASSIFY	SCREEN	ASSESS	ACT
Step 1 Classify the research field Is this a Critical & Key Technology Area (CKTA)?	Step 2 Set risk tolerance Institution or agency declares high, medium, or low tolerance up front.	Step 3 Run four checks Screen all PIs, co-PIs, and funded personnel against checks A–D.	Step 4 Apply cooling-off Period set by finding type and declared risk-tolerance tier.

4.1 Classify: Critical and Key Technology Area (CKTA) vs. Standard Research

Every proposal receiving federal funds runs through the same four checks in Section 4.3, since there is no reliable way to know in advance which specific researchers or collaborations carry entity-list risks. What the CKTA classification determines is how strict the consequences are once a check surfaces a finding.

Critical and Key Technology Area (CKTA) research. Proposals classified as touching a CKTA should belong to a lower risk-tolerance tier, and therefore have a longer cooling-off period, because compromise in that technology area carries greater national security weight. Ideally, what constitutes a CKTA would be tied to a consolidated, cross-agency national list. No such list currently exists. Different statutes and agencies reference overlapping and only partially compatible definitions and lists.

Standard research. A proposal outside a CKTA can reasonably operate under a higher risk-tolerance tier, and a correspondingly shorter cooling-off period, because the stakes of compromise are lower. Section 4.4 develops the cooling-off periods each tolerance tier implies.

Non-CKTA research can still carry dual-use or military end-use potential, which is why every researcher would receive the same four checks in Section 4.3 regardless of CKTA status; only the resulting cooling-off period differs by classification.

4.2 Screen: Declaring Risk Tolerance

Before any proposal is assessed, an institution or agency declares its own risk-tolerance tier for research security (e.g., high, medium, or low). Declaring a tier in advance provides a calibrated rather than discretionary framework: it commits an institution or agency to a consistent standard before any specific finding is in front of it, rather than deciding after the fact how seriously to treat a given researcher or proposal.

Consistent with the Classify step above, the same institution or agency may reasonably declare a lower tolerance tier for CKTA-designated work than for standard, non-CKTA work, since compromise in a CKTA field carries greater national security weight. A declared tolerance may also reasonably

reflect an institution’s own resources and its reliance on federal funding, consistent with the premise this framework rests on: not every institution needs to operate at the same level of rigor. Section 4.4 translates a declared-tolerance tier directly into the cooling-off periods that follow from it.

4.3 Assess: Four Screening Checks

Every PI, co-PI, and funded researcher on a federally funded proposal, CKTA or standard, is screened against the same four standardized checks:

Table 3. Recommended screening checks for all proposals submitted to federal funders.

Check	What It Screens For
A — Entity-list funding	Has the researcher received grants from any entity-list organization in the last 1, 3, 5, or 7+ years? The lookback window is set by institutional or agency guidance.
B — Collaboration with entity-list researchers	Co-authored publications, patents, or clinical trials with entity-list-affiliated researchers, evaluated against a rolling-window threshold (e.g., 3 of the last 5 years) or an output-share threshold (e.g., 25%+ of outputs).
C — Personal entity-list affiliation	The researcher held an appointment or had an employment relationship with an entity-list organization within the relevant lookback period.
D — MFTRP participation	Active participation in a Malign Foreign Talent Recruitment Program — already a statutory bar to funding eligibility under the CHIPS and Science Act.

4.4 Act: Cooling-Off Periods by Risk Tolerance

Once a tier is declared (Section 4.2), it determines how long a cooling-off period applies before federal funding eligibility is restored when an entity-list tie has ended. Federal agencies and research institutions may each independently set this period to reflect the risk tolerance they have declared. The durations below are illustrative, not prescriptive. They provide a starting point institutions and agencies can adapt to their own technology exposure and risk tolerance.

Table 4. Illustrative cooling-off periods by risk tolerance.

	High risk tolerance	Medium risk tolerance	Low risk tolerance
A — Post-divest cooling-off	0–6 months	1 year	2 years
B — Collaboration threshold	0–6 months	1 year	2 years
C — Active / recent affiliation	2 years	2 years	2 years + no PI role

D — MFTRP participation: automatic ineligibility at every tolerance tier. This is mandated by the CHIPS and Science Act, not a matter of institutional discretion. An additional cooling-off period following MFTRP participation is a reasonable safeguard but is not yet codified in statute.

4.5 Institutional-Level Controls

The four checks above operate at the level of the individual researcher. Section 3.5 showed why that is not enough on its own. During the time a visiting scholar is embedded in a U.S. lab or department, their affiliation is the U.S. institution that is hosting them, not their home-country entity-list affiliation. An individual-level check would not flag anything when the collaboration is taking place. Because of the existing federal policy gap addressing transient researchers, funders and institutions should consider extending their risk calibration to the department or lab level: a department with a documented history of hosting entity-list-affiliated visiting scholars in a CKTA field has a different risk profile than one with no such history.

Proportionate, department-level controls consistent with this framework may include:

- Restricting open seminars, lab tours, and informal data or equipment access on actively funded CKTA research within departments that have a documented history of entity-list-affiliated visiting scholars.
- Requiring visiting-scholar sponsors in those departments to complete an additional data-handling and export-control briefing before a visitor’s appointment begins.
- Applying a shorter, mandatory data-access review window for short-term appointees working on CKTA-designated grants, regardless of the visitor’s home-country affiliation. The review is triggered by appointment length and technology area, not nationality.

4.6 Policy Gaps and Recommendations

Applying this framework surfaces five gaps in the current federal research security policy landscape that limit consistency and defensibility for both funders and institutions:

Table 5. Policy gaps in the current federal research security landscape and accompanying recommendations.

Policy Gap	Recommendation
No unified national CKTA list	A single, regularly updated, cross-agency national list naming each CKTA, paired with a clear definition for each, would give researchers, institutions, and agencies a shared, consistent reference for determining whether a given proposal qualifies as CKTA research.
No federal cooling-off framework for researchers	Revolving-door rules govern former federal employees moving into the private sector, but no equivalent framework exists for researchers re-entering federal funding after an entity-list affiliation. Cooling-off periods may be a helpful model for institutions and federal agencies to adopt: they would give researchers and institutions a clear, predictable answer to what to expect after an entity-list affiliation, and when eligibility for federal funding resumes.
Inconsistent collaboration thresholds	Standardizing a rolling-window metric (e.g., collaboration in 3 of the last 5 years, or 25%+ of outputs) across agencies would reduce arbitrage between funders and institutions.
Undefined re-entry pathways	Researchers who divest from an entity-list tie do not have clarity on how it impacts their federal funding eligibility going forward. A defined, transparent cooling-off period would give both researchers and institutions the clarity to weigh the risk and its consequences, rather than not knowing where they stand until a specific case forces the question.
One-size-fits-all mandates misallocate risk	Uniform requirements treat all research institutions identically. A risk-calibrated framework would, instead, let each institution weigh, based on its own exposure, risk tolerance, and reliance on federal funding, whether investing in a high level of research security rigor makes sense for them.

5. Conclusion: Toward Proportionate Vigilance

Much of the pushback against research security policies comes from the fear that they will erode the openness that made U.S. science preeminent, and with it, the country's competitive edge as a scientific power. This is often juxtaposed against a different view that certain foreign nations are actively exploiting U.S. openness to advance their own capabilities. This report shows that even though the risk is real, it is narrow and concentrated, with roughly 1 in 70 U.S.-affiliated researchers having an entity-list tie.

This report measures research security exposure through international collaborations and entity-list affiliations. Exposure does not mean that a given collaboration or affiliation resulted in the “detriment of national or economic security, related violations of research integrity, and foreign government interference” as specified in NSTC's definition of research security, only that the underlying activity made some degree of knowledge or IP transfer likely.

It is possible to choose both scientific openness and security. Doing both well means applying the same baseline screening to every researcher and proposal, while directing the strictest consequences and longest cooling-off periods toward research areas that carry the greatest risk to the United States, critical technology areas like quantum computing, artificial intelligence, and biotechnology, rather than applying a one-size-fits-all approach that is either too restrictive or too trusting.

Transient researchers present a research security policy gap: current disclosure forms ask about a collaborator's affiliation, but a visiting scholar's affiliation of record is the same U.S. institution the PI is at. Their status as a visitor and their home-country affiliation never have to appear on the form at all. No federal policy currently addresses this gap directly. Because individual-level checks cannot catch this pattern while it is happening, the more useful signal may sit one level up: a department or lab with a documented history of hosting entity-list-affiliated visiting scholars in a critical technology area carries a different risk profile than one with no such history. Until federal policy addresses this gap, it is up to individual research institutions to decide what safeguards, if any, they want in place for how their departments and labs engage visiting scholars and short-term appointees.

Research security works only as a shared responsibility model. The researcher retains the primary duty to disclose completely and accurately. The institution is the first line of defense: it must verify disclosures using available research security tools, including cross-checks against external data, before a proposal is submitted, rather than treating disclosures as a compliance checkbox and passing along whatever a researcher provides. The funding agency is the second line of defense, screening before an award is made rather than after. And enforcement (e.g., the False Claims Act, and DOJ action more broadly) should be the last line of defense in this system. Every dollar recovered through litigation is a dollar that was already spent, and likely represents IP or knowledge that was already transferred. The risk-calibrated framework in Section 4 offers a starting point for institutions and agencies to decide how much to invest in research security, calibrated to their own risk tolerance.

Appendix: Methodology and Data Limitations

Scope and Data Sources

All data were drawn from the Dimensions database. Publications, grants, researchers, and organizations were linked through consistent identifiers rather than through name-matching, so a given researcher, institution, or funder resolves to the same underlying record wherever it appears, without the false-positive risk that comes from matching on names alone. Researcher identifiers are resolved conservatively within the database: when it cannot be confidently determined that two same-named authors are the same individual, they are kept as separate profiles rather than merged, and this reference data is updated on a periodic basis. This means that a single researcher’s record is more likely to be split across two profiles than to wrongly merge two different people into one, which would bias this report’s counts toward undercounting exposure rather than overstating it.

A publication or grant is treated as federally funded if at least one of its funding organizations belongs to the curated “U.S. Federal Funder” group within the Dimensions database. Organizations are treated as entity-listed if they appear on any of the restricted-entity lists in Table 6; where an organization appears on more than one list, it is counted once in pooled totals.

Restricted-Entity Lists Referenced in This Analysis

“Entity-list affiliation” refers to an author, institution, or funding acknowledgment matched to an organization appearing on one or more of the following lists.

Table 6. Restricted-entity lists used in this analysis.

List	Maintained By / Scope
U.S. BIS Entity List	Dept. of Commerce (Bureau of Industry and Security). Export-control restricted parties, cross-sector.
U.S. NDAA §1260H list	Department of Defense. Chinese military companies.
U.S. NDAA §1286 list	Department of Defense. Foreign institutions of higher education engaged in problematic research activity (China, Russia, Iran, and other flagged jurisdictions); most recently updated for FY2025 in June 2026.
U.S. NDAA §5949 list	Federal Acquisition Regulation, under §5949 of the FY2023 NDAA. Prohibits federal agencies from procuring semiconductor parts, products, or services traceable to specific named Chinese companies (currently SMIC, CXMT, and YMTC).
U.S. NDAA §889 list (“McCain 889”)	Federal Acquisition Regulation, under §889 of the FY2019 NDAA. Prohibits federal agencies, contractors, and grant recipients from procuring or using covered telecommunications or video-surveillance equipment from a named set of Chinese companies.
“Seven Sons of National Defense” universities	Informal designation for PRC universities with close R&D ties to the People's Liberation Army; commonly cross-referenced alongside the NDAA §1286 list.
U.S. FCC Covered List	Federal Communications Commission, under the Secure and Trusted Communications Networks Act of 2019. Telecommunications and video-surveillance equipment and services deemed a national security risk; bars use of USF subsidies and new equipment authorizations.

List	Maintained By / Scope
U.S. UFLPA Entity List	Dept. of Homeland Security (Forced Labor Enforcement Task Force). Entities linked to forced labor in China's Xinjiang region; a different rationale (forced labor, not technology transfer) than the other lists in this table.
U.S. Treasury OFAC SDN List	Dept. of the Treasury (Office of Foreign Assets Control). Specially Designated Nationals; general sanctions, not research-specific.
U.S. Treasury OFAC Consolidated Sanctions List	Dept. of the Treasury. Broader consolidated sanctions designations.
U.S. Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC) List	Dept. of the Treasury (OFAC), under Executive Order 14032. Bars U.S. persons from trading publicly traded securities of listed Chinese military-industrial complex companies; narrower than the SDN or Consolidated lists.
UK Sanctions List	United Kingdom government.
EU Consolidated List	European Union.
Australia Consolidated List	Government of Australia.
Canada's Named Research Organizations List	Government of Canada.

Key Definitions and Parameters

Several terms carry a specific, deliberately chosen meaning throughout this report:

- **U.S.-affiliated researcher:** a researcher who carries at least one U.S.-based organizational affiliation on a given publication. Researchers are tracked using Dimensions' disambiguated researcher identifiers; author mentions that cannot be matched to a disambiguated identifier are excluded, so an individual is counted consistently across publications and grants rather than once per name variant.
- **Flagged researcher:** a U.S.-affiliated researcher who also carries at least one entity-list affiliation within the same calendar year.
- **Transient researcher:** a flagged researcher whose U.S.-affiliated publication record spans 24 months or less, used as a proxy for visiting-scholar or short-term-appointment status rather than a direct appointment-record match.
- **International collaboration (Section 3.3):** a publication counts as an international collaboration if it has at least one U.S.-affiliated author and at least one non-U.S. co-author. A publication is an international entity-list collaboration if the co-author is affiliated with an entity-list organization. The reported percentage uses all internationally co-authored, federally funded publications as its denominator (not all funded publications overall) so the metric reflects the share of international collaboration that involves an entity-list collaborator.
- **Federal funding received after an entity-list affiliation (Section 3.4):** a grant counts as received after an entity-list tie only if its start year falls strictly after the year of that researcher's most recent entity-list affiliation. Same-year cases are deliberately excluded. This report tested a same-year-or-after threshold as an alternative and chose the stricter approach: a research proposal may sometimes be

submitted six months to a year or more before an award is made, and the publication that would reveal an affiliation to an outside observer may not appear until well after that affiliation began, given typical publication lag. A same-year tie may, therefore, not yet have been findable by a funding agency at the time it made an award. Requiring the affiliation to be strictly in the past isolates cases where the tie was already part of the public record, meaning a federal agency reviewing the same external data used in this analysis could plausibly have found it before the award was made. The same-year-or-after threshold was tested and produced a similar overall pattern, but the stricter definition is used as the primary, more defensible measure.

- **Duration of U.S. affiliation (Section 3.5):** calculated from the number of distinct years a flagged researcher held a U.S. affiliation on federally funded publications specifically, not their broader publication record.
- **Cooling-off period (Section 4.4):** the length of time that must elapse after a triggering entity-list condition ends before a researcher is eligible for new federal funding, with duration scaled to an institution's or agency's declared risk-tolerance tier and to whether the research is CKTA-classified (Section 4.1). Illustrative durations appear in Table 4.

Counting and Deduplication

All counts in this report are deduplicated at the appropriate level: a single publication, researcher, or grant is counted once regardless of how many funders, authors, or affiliations it lists internally. Grant funding totals are summed over distinct grants, so a single grant shared by multiple researchers is not counted multiple times. Where a figure reports a count "per year," the same researcher can appear in more than one year's count; where a figure reports a total "across the full period," each researcher is counted once for the entire decade. The two are not directly comparable to one another.

Limitations

As described above, the conservative approach to researcher identity means some individuals (e.g., those with common names, limited identifier coverage, or short publication histories) may be split across multiple profiles rather than merged into one; this is expected to undercount exposure rather than overstate it. Publication and grant-record data are also subject to an inherent reporting lag: articles pass through submission, acceptance, and indexing before appearing in bibliometric databases, and grant records may be updated or amended after initial disbursement. As a result, figures for 2024 and especially 2025 likely understate true research activity and should be interpreted as a lower bound rather than a precise count; the apparent volatility in flagged-researcher counts in the most recent two years should be read with this caveat in mind rather than as a confirmed reversal or improvement in trend (see Section 3.6).

Entity-list and U.S.-affiliation matching in this report both depend on an author affiliation being resolved to a GRID organization level, consistent with how the underlying restricted-entity lists in Table 6 are themselves structured as named-organization lists rather than country lists. An affiliation that cannot be resolved to a GRID identifier (for example, due to incomplete address metadata or an organization not yet indexed in GRID) is excluded from both the U.S.-affiliated research population and entity-list matching, rather than being included based on a country code alone. Because GRID resolution is a precondition for both sides of these calculations, the absolute counts reported throughout this report (e.g., total U.S.-affiliated researchers, flagged researchers, dollars funded) should be read as a floor. The share-based figures (e.g., percentage of publications or researchers flagged) are less straightforwardly biased in one direction and are best read as estimates conditional on GRID coverage rather than as a strict lower or upper bound.

Furthermore, entity-list status in this report reflects the state of the restricted-entity reference data used in the analysis (conducted August 4, 2026), not the date an organization was actually added to a list. Underlying publication, grant, and entity-list tables are queried live from continuously updated Dimensions data in Google BigQuery (GBQ) rather than a static, versioned extract; re-running the same query logic at a later date is expected to produce figures that differ slightly from those published here, reflecting ongoing indexing and list revisions rather than a change in methodology. A publication from early in the study window involving an organization added to a list years later is still counted as an entity-list affiliation in this report's pooled totals. Determining the precise list-membership date for every organization across every list was outside the scope of this analysis. This means the analyses in this report describe exposure under today's list definitions applied retrospectively, not a real-time historical record of how risk would have appeared at the time.

This report measures research security exposure against the restricted-entity lists in Table 6. An organization that is not on an entity list in Table 6 may still present a research security risk; collaboration or affiliation with such organizations would not be captured in this report. The figures in this report should accordingly be read as a measure of exposure to already-designated entities specifically, not as a comprehensive measure of research security risk across the research ecosystem as a whole.

Grant and publication timing in this analysis is resolved to the calendar year, not the specific date. As a result, this analysis cannot determine whether a same-year grant and a same-year entity-list affiliation occurred in a particular sequence within that year.

Framework Status

The risk-calibrated framework in Section 4 is a policy proposal synthesized based on the current federal disclosure practice and the evidence presented in this report. With the exception of Check D (MFTRP participation, which is a statutory bar under the CHIPS and Science Act), none of the specific thresholds, lookback windows, or cooling-off periods described are currently codified in law or federal regulation. They are offered as a starting point for institutional and agency policy design, to be adapted to an organization's own technology exposure and risk tolerance.

Report

Han, X. (2026). *Research security in U.S. federally funded science: Evidence, exposure, and a risk-calibrated path forward*. Digital Science Insights. <https://doi.org/10.6084/m9.figshare.33995349>

Dataset

Han, X. (2026). *Research security in U.S. federally funded science: Evidence, exposure, and a risk-calibrated path forward* [Data set]. Digital Science. <https://doi.org/10.6084/m9.figshare.33995364>

Your Research. Our Mission.

In an era of shifting research landscapes and increasing security concerns, government agencies are challenged to identify, fund, and manage high-impact research programs effectively. From diminishing funding to threats posed by bad actors, the integrity and security of national research initiatives are under unprecedented scrutiny.

Digital Science provides national government departments with secure research intelligence solutions to support national research security, technology foresight, and strategic investment decisions. Meaning that you can focus on the insights that matter, reduce manual analysis, and build stakeholder confidence.

Our integrated solutions help you to easily spot risk, identify opportunity, and support your work across the global research landscape.

Secure research platform to maintain data integrity.

We provide the essential tools to manage critical research security risks, ensure data integrity, and maintain a competitive edge. Our focus is on delivering trusted, transparent research intelligence that aligns with your agency's mission.

- **Safeguard your research programs against foreign influence:** Detect hidden R&D risks before they compromise your operation. Map sensitive collaborations, monitor funding and institutional relationships, and protect your research base while enabling responsible global collaboration.
- **Track emerging technology and fund the future of research:** Strengthen your research outcomes by identifying emerging topics, trends, and technologies and assessing their potential impact.
- **Accelerate research outcomes with AI:** Leverage AI to increase efficiency when making your strategic decisions, saving time so you can focus on your impact across the research landscape.

Secure and intelligent solutions for government agencies

Digital Science for Government is your intelligence partner across the research ecosystem. We are here to help you advance research faster and make smart, data-driven decisions with confidence.

Learn how Digital Science can help you identify, fund, and manage the research of tomorrow.



digital-science.com