

How to Stop China's Theft of Taxpayer- Funded Research

The Reforms We Need and Rebuttals to
Those Who Oppose Them

THE SELECT COMMITTEE ON THE
STRATEGIC COMPETITION BETWEEN
THE UNITED STATES AND
THE CHINESE COMMUNIST PARTY



Assessment of Common Arguments Used to Oppose Strengthened Research Security Measures

Since initiating its investigations into research security failures across institutions of higher education, the federally funded research ecosystem, and executive branch agencies, the Select Committee on China (the Select Committee) has repeatedly encountered a familiar set of arguments opposing stronger safeguards and downplaying the severity of research security threats. These arguments—often advanced by universities, academic and university associations, lobbying organizations, and portions of the broader federally funded research and policy community—are often presented as principled defenses of academic openness, scientific collaboration, or administrative practicality. In reality, many of these arguments are flawed, incomplete, detached from the operational realities of how research is conducted and exploited by foreign adversaries, or ignore the empirical evidence gathered through years of federal investigations,^{1,2,3} criminal and civil prosecutions,⁴⁻²³ publicly available intelligence reporting,^{24,25,26,27} think tank analysis,²⁸⁻³⁶ investigative journalism,³⁷⁻⁴¹ assessments by allied foreign government entities,^{42,43,44} suspensions and debarment records,⁴⁵ literature from subject matter experts,^{46,47} and congressional oversight investigations.⁴⁸⁻⁵⁷

The arguments and underlying claims against research security safeguards deserve greater scrutiny for several important reasons.

First, many of the claims have become institutionalized within portions of academia, federal grant-making agencies, scientific associations, and lobbying organizations. They are frequently repeated in policy debates, congressional testimony, media engagements, and public statements as though they are settled truths, despite often lacking evidentiary support.

Second, the arguments often present a false binary between openness and security. The United States can maintain a vibrant and innovative research ecosystem while also imposing targeted safeguards designed to prevent adversarial exploitation. Openness does not require the absence of rules, oversight, or accountability. Nearly every other domain involving national security-sensitive and dual-use technology activity operates with some form of risk management, compliance structure, vetting, or restriction. Federally funded research should not be treated as uniquely exempt from such protections, particularly when highly motivated foreign adversaries like China explicitly target it for acquisition and exploitation.

Third, many objections to strengthened research security measures rely on theoretical concerns while ignoring documented evidence of harm. The Select Committee's investigations, along with numerous federal criminal cases, intelligence assessments, inspector general findings, think tank reports, investigative journalism, foreign government analysis, and Executive Branch agency reports demonstrate that the People's Republic of China (PRC) has systematically leveraged academic collaboration, joint research, talent recruitment programs, undisclosed affiliations, co-authorship networks, and open research

environments to advance its military modernization, strategic industries, and technology acquisition objectives.

Fourth, some arguments opposing stronger safeguards reflect a misunderstanding of how the PRC's military-civil fusion (MCF) strategy functions in practice. Under MCF, distinctions between civilian and military entities are intentionally blurred. Universities, state laboratories, commercial companies, and ostensibly civilian researchers may all contribute directly or indirectly to the PRC's defense-industrial base and military modernization objectives. Traditional assumptions that civilian research collaboration is inherently benign are increasingly outdated and incompatible with the realities of China's state-directed technology acquisition system.

Finally, many of these arguments improperly frame research security measures as "anti-science", "anti-collaboration", or "anti-international engagement." The purpose of research security safeguards is not to eliminate international collaboration or undermine scientific progress. Rather, the purpose is to ensure that taxpayer-funded research does not directly or indirectly support foreign military advancement, human rights abuses, strategic competitors, or entities acting contrary to U.S. national security interests.

* * * *

To provide greater transparency into the factual record underlying this report, the Select Committee is releasing hundreds of pages of previously non-public, unclassified investigative records concerning research security cases investigated by the National Science Foundation Office of Inspector General (NSF OIG). These records include investigative reports, suspension and debarment recommendations, correspondence, foreign employment and talent-program records, financial information, disclosure documents, and other supporting materials collected during federal investigations.

These documents provide an important window into what research security failures actually look like in practice. They show that many cases involve substantially more than technical mistakes or isolated failures to complete paperwork. The records document undisclosed foreign positions and affiliations, foreign income and research support, participation in PRC talent recruitment programs, outside employment, conflicts of commitment, and repeated omissions from federally required disclosures. In some cases, the conduct extended across multiple years, institutions, awards, and federal agencies. For example, NSF OIG records concerning one senior university researcher documented undisclosed PRC university positions, income, research support, and participation in the Thousand Talents Program and 111 Project, with omissions in NSF proposal documents dating back years. Investigators described the conduct as a pattern involving repeated failures to disclose foreign affiliations, funding sources, and salary payments.

The Select Committee is releasing these records because the debate over research security should be grounded in evidence rather than abstractions. Many of the arguments examined in this report—including claims that disclosure failures are merely administrative errors, that existing self-policing mechanisms are sufficient, or that stronger safeguards are unnecessary—can be evaluated against the contemporaneous records developed by federal investigators. The documents therefore serve as part of the evidentiary foundation for the analysis that follows. Where relevant, this report draws directly from these records to test commonly asserted arguments against the facts identified through actual investigations and to illustrate the vulnerabilities that federal research security safeguards are intended to address.

SECTION 1: FALSE PREMISE ABOUT RESEARCH RELATIONSHIPS

1. Co-authorship vs. Collaboration

Co-authored publications are the visible output of a broader process that often includes data sharing, methodological input, iterative feedback, and ongoing technical exchange. The claim that co-authorship does not equate to collaboration is a distinction without meaningful difference. While it is technically true that not every co-author engages at the same level or in the same way, this argument ignores how modern research is conducted. Co-authorship reflects a research relationship that exists on a spectrum rather than as a binary distinction.

At one end, it may involve close, sustained collaboration with shared experimental design, data exchange, and iterative problem-solving. At the other, it may reflect more limited contributions, such as discrete analysis, validation, or technical input. But in all cases, co-authorship signifies some level of intellectual participation. These interactions frequently occur outside the final published record, yet they are precisely where sensitive knowledge, early-stage insights, and tacit expertise are most likely to be transferred. Treating co-authorship as disconnected from collaboration disregards the cumulative and networked nature of research activity.^a

Many publications include detailed author contribution statements precisely to clarify each individual's role, whether in conceptualization, methodology, experimentation, data curation, analysis, writing, or editing. Co-authorship reflects more than a passive acknowledgment of contribution. These disclosures underscore that authorship is tied to defined participation in the research process, not incidental association. Even when contributions differ in scope or depth, inclusion as a co-author signals engagement with the underlying work.

It confers legitimacy and expertise, signals a working relationship, and demonstrates inclusion in a shared research effort. In many cases, co-authored work is supported by overlapping funding streams, shared infrastructure, or coordinated lines of inquiry. Even where direct interaction may be limited, the integration of U.S. taxpayer-funded research into joint outputs that include foreign entities, particularly those tied to adversary governments, creates clear pathways for knowledge transfer and amplification.

It also confers legitimacy on those entities by associating them with U.S.-funded work and experts, enhancing their credibility, visibility, and ability to attract

^a However, an important exception arises in cases of “hyper-coauthorship,” such as large-scale particle physics or astrophysics collaborations involving dozens or even hundreds of authors. In these instances, authorship is often spread out and does not reflect meaningful research relationships between individual contributors or institutions, limiting its value for assessing collaboration or risk. Accordingly, such publications should be excluded from research security analyses, as they provide little actionable insight into substantive engagement between entities.

additional partnerships, funding, and talent. From a research security perspective, the relevant question is not just whether every author collaborated equally, but whether the research ecosystem itself enables the flow of sensitive capabilities, expertise, or credibility to high-risk actors.

If co-authorship is dismissed as incidental or non-substantive, it raises a separate question: why are individuals or institutions listed as authors at all? Authorship carries professional, academic, and reputational weight. It is used to justify promotions, secure funding, and establish technical authority. If contributors did not meaningfully participate, their inclusion is not benign; it is a misrepresentation of contribution and a potential breach of academic standards and integrity. **Institutions that assert co-authorships are not indicative of collaboration cannot simultaneously rely on those same publications as evidence of scholarly output and impact.**

According to multiple law enforcement officials, law enforcement has long relied on publication data, including co-authorship, as a foundational investigative tool.⁵⁸ Over the past decade, agents have used bibliometric analysis to generate leads in cases involving undisclosed financial ties, hidden foreign affiliations, and unreported research relationships.⁵⁹ Patterns in co-authorship, institutional linkages, and publication acknowledgments often provide the first visible indicators of relationships that were not properly disclosed through official channels. These data points have supported not only preliminary inquiries but also criminal, civil, and administrative investigations.

Publication records are one of the most transparent and accessible sources for mapping research networks and identifying potential risk vectors. In many cases, publication data has been incorporated into affidavits supporting search warrants, one of the highest legal thresholds in law enforcement. The use of such information at that level underscores its evidentiary value and credibility. Numerous Department of Justice (DOJ) indictments and civil settlements and fact-based suspensions and debarments over the past ten years have drawn, in part, on publication records and co-authorship patterns to establish undisclosed relationships.⁶⁰

These dynamics are further reinforced by the structure of PRC research and talent recruitment programs, which explicitly incentivize and, in many cases, require co-authored publications. Chinese research and employment contracts routinely mandate that researchers publish high-quality papers, often in collaboration with domestic institutions.⁶¹ Talent program agreements have gone further, requiring principal investigators to publish multiple papers with PRC-based instructors and graduate students as co-authors.⁶² These provisions are not benign academic expectations; from the PRC's perspective they are mechanisms designed to formalize and expand collaborative ties, embed foreign expertise within PRC research ecosystems, and generate tangible outputs that demonstrate integration.

Co-authorship is a critical indicator within a broader pattern of activity that includes funding sources, institutional affiliations, known ties to foreign

defense ecosystems, and the subject matter of the research itself. Dismissing co-authorship as irrelevant or insufficient on its own is an attempt to narrow the aperture of analysis in a way that obscures risk. When evaluated alongside other available data, co-authorship remains one of the most accessible and revealing indicators of research relationships that may carry national security and fraud implications.

The NSF Office of Inspector General's investigation into University of Tennessee professor Dr. Bin Hu demonstrates how publication records served as a critical evidentiary component in mapping undisclosed relationships with PRC institutions, identifying overlap between federally funded U.S. research and Chinese government-funded projects, corroborating foreign affiliations, and linking publications to undisclosed foreign funding streams. Investigators identified dozens of publications citing both U.S. federal funding and PRC funding sources, publications listing dual affiliations with U.S. and Chinese institutions, and publications acknowledging PRC grants that had not been properly disclosed to U.S. funding agencies. The investigation further found that publication acknowledgments and overlapping project titles helped establish connections between NSF-funded work and parallel PRC-funded research projects, contributing to the eventual recommendation for government-wide debarment (See Appendix A).⁶³

When universities engage in research with high-risk or defense-affiliated foreign entities, there can be real reputational consequences, due to the visibility in the public record. Co-authored publications serve as a permanent, searchable ledger of these relationships, exposing institutions to scrutiny from Congress, federal agencies, law enforcement, and the broader public. Public publication records shape perceptions of institutional judgment, governance, and integrity. Moreover, by lending their name, expertise, and federally supported research to such relationships, institutions confer legitimacy on those entities, amplifying their global standing while simultaneously degrading their own. In an environment where publication data is routinely used by investigators, policymakers, and oversight bodies to identify undisclosed relationships and compliance failures, universities cannot assume these partnerships will remain obscure or inconsequential.

Lastly, universities cannot have it both ways. They cannot claim superior insight into research relationships while simultaneously relying on or tolerating inaccurate disclosures in the published record. Maintaining non-public knowledge of author contributions that is not accurately reflected in federally funded publications amounts to *de facto* concealment of the true nature of research relationships. Such practices undermine the credibility of the research enterprise and the integrity standards universities should uphold. Ultimately, universities and researchers have used this argument as a rhetorical device to downplay risk and avoid accountability.

2. Researchers are Added to Publications Without their Knowledge

The assertion that researchers are added to publications without their knowledge is not a credible defense. It is an admission of a breakdown in research integrity, authorship accountability, and institutional oversight. Established guidelines, including those from most major journals, require that authors make a substantive intellectual contribution, participate in drafting or revising the work, approve the final version, and accept accountability for its contents. Being listed as an author is not ceremonial. It is a formal certification of contribution and responsibility.

Additionally, author disclosure practices in publications in some cases are inconsistent and often lack standardization. Some papers include detailed author contribution statements and clearly identify funding sources with specific grant numbers tied to individual researchers, while others provide only vague acknowledgments (e.g., “supported by NASA” or a general program reference) without grant identifiers or attribution of funding to specific co-authors.

If individuals are being added without their knowledge, then one of two things is true, and neither is acceptable. Either the authorship process is being manipulated in a way that undermines the credibility of the research, or the individual is aware and later denies involvement when scrutiny arises. Both scenarios cut directly against the principles of transparency and integrity that universities publicly espouse. Faculty routinely rely on their publication record for career advancement, grant applications, federal funding proposals, awards, and professional recognition. Universities themselves use these outputs to justify funding, rankings, and institutional prestige. One cannot simultaneously claim that authorship is meaningless or accidental while continuing to derive professional and financial benefit from those same publications.

If a researcher truly did not materially contribute to the research and was added without consent, then the academic integrity and ethical obligation is clear. The scholarly record must be corrected. That means notifying the journal, removing the individual from authorship, and issuing a formal correction or retraction as appropriate.

Institutions cannot selectively invoke research and academic integrity. If they espouse transparency, accountability, and accuracy in the scholarly record, then they must be willing to enforce those principles even when it is inconvenient. That includes retracting or correcting publications where authorship is improper and ensuring the record accurately reflects who performed the work.

3. “Fundamental Research is Openly Published; Thus, Restricting any Collaboration is Pointless Since the Research will be Shared Broadly and Internationally”

Open publication does not mean equal access to knowledge. The premise of that argument is flawed because it treats published research as the full value of scientific work, when in reality it is only the final output of a much larger and more

valuable process. What is published is a distilled, sanitized version of the work. It captures conclusions, selected methodologies, and results. It does not capture the full body of tacit knowledge generated during the research lifecycle: failed experiments, parameter tuning, workarounds, troubleshooting decisions, informal exchanges between collaborators, lab techniques, data conditioning choices, or the iterative reasoning that led to the final outcome. Those elements are often far more valuable than the paper itself because they dramatically reduce the time, cost, and uncertainty required to replicate or extend the research.

Not all actors operate under the same constraints. State-directed systems, particularly those pursuing military-civil fusion strategies like China, are structured to rapidly absorb, adapt, and operationalize openly available research in ways that U.S. institutions often cannot or will not. The issue is not whether information is technically accessible. It is how efficiently and for what purpose it is exploited.

A further flaw in this argument is the assumption that fundamental research remains confined to the open domain. In practice, that is not how the U.S. research and development ecosystem operates. **In some cases, federally funded fundamental research, including work supported by the Department of War, serves as the foundation for subsequent applied, controlled, or classified efforts. Early-stage discoveries may transition into sensitive programs, including controlled research, classified initiatives, and, in some instances, Special Access Programs that directly support warfighting capabilities.** The initial “fundamental” phase is therefore not an endpoint, but part of a broader development pipeline. Allowing foreign entities, particularly those tied to adversarial governments, to participate at the front end of that pipeline provides them with significant insights and hands-on knowledge into technologies that may later underpin sensitive or classified capabilities. By the time such work transitions out of the open domain, the foundational knowledge and technical expertise have already been shared. Restricting some research relationships with certain entities at the early stages is not about limiting open science. It is about protecting the upstream inputs that ultimately enable downstream military and strategic advantages.

Finally, if research relationships truly added no value beyond what is already published, there would be no reason to pursue it so aggressively. Yet foreign entities, particularly those tied to strategic competitors, consistently seek collaborative arrangements, joint labs, visiting researcher positions, and co-authorship opportunities. They do so precisely because collaboration provides access to the non-public, high-value aspects of research that publications do not capture.

SECTION II—CLAIMS ABOUT BENEFITS, RISK, MITIGATION, AND SELF-POLICING

4. **“The United States Derives Greater Benefit from Research Relationships with China than China Derives from the United States, and Therefore Restrictions on Research are Unnecessary”**

The claim that the United States benefits more than China from scientific collaborations is, at this point, an assertion rather than an empirically established fact. In the context of U.S. government-funded research, that is not a trivial distinction. If proponents want to argue that unrestricted collaboration with Chinese defense research and industrial base entities produces net benefits for the United States, then they should be required to demonstrate that with evidence, not rhetoric. There is a substantial and growing body of evidence, including court cases, indictments, investigations, compliance reviews, suspensions and debarments, congressional reports, think tank analyses, and both quantitative and qualitative research that provide empirical evidence on how China exploits U.S. research and academia. This evidence spans not only the United States but also allied and partner nations around the world.

The burden of proof rests with those arguing against restrictions. That is especially true where the collaboration involves U.S. taxpayer-funded defense research and institutions tied to a strategic competitor’s military, defense industrial, or state-directed technology transfer ecosystem. It is not enough to vaguely suggest that scientific exchange is mutually beneficial or that American researchers “learn something too.” What matters is whether there is concrete, documentable evidence showing that these collaborations generated unique, material, and operationally relevant benefits for the United States that could not have been obtained through domestic research, allied partnerships, or other lower-risk channels.

All of us should demand the same rigor here that science demands elsewhere. If someone makes the claim that these research relationships produced meaningful benefits for the United States, they should be able to produce evidence that is specific, measurable, and capable of scrutiny:

What exactly did the PRC collaborator provide? What was truly unique about it? Why could it not have been obtained elsewhere or from a trusted partner? Did the Chinese co-author or institution provide unique data, specialized materials, proprietary methods, access to equipment, or some other indispensable contribution the U.S. side did not already possess or could not independently acquire? Was the U.S. researcher given access to Chinese defense laboratories, facilities, or technical capabilities that materially changed the outcome of the work?

There is also a deeper flaw in the argument. It assumes that the relevant metric is whether the United States got something out of the collaboration. That is too

low a bar. The real question is whether the United States got enough unique benefit to justify the transfer of knowledge, access, legitimacy, and relationship-building that the collaboration simultaneously provided to entities tied to China's defense ecosystem.

Even if a U.S. researcher gained something of marginal value, that does not mean the exchange was prudent or advantageous overall. A collaboration can produce some academic benefit for the American side while still delivering far greater strategic value to the Chinese side. Those are not mutually exclusive. In fact, that is often the central risk.

This is particularly important because the benefits flowing to authoritarian regimes such as China are not limited to what appears in the publication itself. Chinese defense-linked entities may gain access to tacit knowledge, insight into experimental design, troubleshooting approaches, early-stage findings, and sustained professional relationships with U.S. researchers and laboratories. They gain credibility through co-authorship, proximity to U.S. institutions, and opportunities for future engagement. Those benefits are diffuse, cumulative, and often difficult to quantify, but they are real. By contrast, proponents of unrestricted collaboration tend to describe U.S. benefits in abstract and anecdotal terms while ignoring the broader and more systemic advantages conferred on the foreign side.

The argument also fails to account for alternatives. Even if some collaborations produced useful information, that does not mean those benefits required collaboration with Chinese defense-linked entities. The relevant question is not simply whether the collaboration yielded something valuable. The relevant question is whether the same or better result could have been achieved through domestic capability, allied partnerships, commercial procurement, open literature, or collaboration with institutions that do not present the same national security risks. If the answer is "yes," then the claimed benefit does not justify the risk.

In other words, the appropriate standard is not whether any benefit was obtained, but whether the collaboration produced unique, significant, and otherwise unavailable value, and whether that value outweighed the known risks of conducting U.S. government-funded research with entities tied to a strategic competitor's defense ecosystem.

5. "Risk Mitigation Alone Solves the Problem — Therefore Prohibitions Are Unnecessary"

Another common argument is that individualized risk mitigation measures are always preferable to categorical prohibitions, and that any problematic research relationship can supposedly be managed through tailored compliance controls rather than outright restrictions and prohibitions. While risk mitigation is an important component of research security, this argument incorrectly assumes that all risks are manageable and that mitigation measures are equally effective across all threat environments. It also ignores the administrative and operational burdens associated with managing high-risk collaborations, often treating those burdens as

though they impose no meaningful cost on the research process. In reality, there are certain entities, institutions, and threat environments where the level of risk is so substantial that meaningful mitigation would require controls so extensive that the collaboration itself becomes impractical, scientifically distorted, or fundamentally inconsistent with the openness and efficiency academia claims to value.

Effectively, what this means is that the level of mitigation required for collaborations involving extremely high-risk entities may itself begin to harm the scientific process by forcing researchers to navigate burdensome restrictions, segmented research activities, limitations on information sharing, and constant compliance oversight. In cases where collaborations would require such extraordinary mitigation measures due to the nature of the entities involved, prohibiting those collaborations altogether and instead directing federally funded research toward domestic or lower risk partners would likely represent a far more practical, secure, and scientifically coherent approach.

The argument also overlooks the fact that risk mitigation is not binary. Some risks can be reasonably managed through disclosures, conflict management plans, publication review mechanisms, cybersecurity controls, stipulating one cannot conduct research with “X” entity, or limited oversight requirements. However, collaborations involving foreign military organizations, national defense laboratories, sanctioned entities, intelligence-linked institutions, or organizations tied to state-directed military-civil fusion efforts present a fundamentally different category of risk. In such cases, the federal government is not dealing merely with minor concerns about transparency or administrative compliance. Rather, it is confronting sophisticated state-backed entities whose institutional purpose may include acquiring foreign technology, advancing military modernization, supporting strategic weapons development, or leveraging civilian research relationships for national strategic objectives.

Additionally, the “mitigation over prohibition” argument often assumes an unrealistic level of institutional capacity and enforcement capability. Effective risk mitigation requires sustained monitoring, technical expertise, institutional discipline, independent verification, and ongoing enforcement over the life of the collaboration. Yet many universities and federal agencies claim to struggle to adequately monitor disclosures, track co-authorship networks, verify foreign affiliations, or conduct meaningful post-award oversight. The assumption that institutions can reliably manage highly sensitive collaborations involving sophisticated foreign military-linked entities through individualized mitigation plans ignores the practical limitations of existing compliance infrastructures.

The argument also fails to account for the cumulative nature of strategic technology acquisition. **Even where no single collaboration transfers a complete technology or classified capability, repeated exposure to research methodologies, tacit knowledge, engineering processes, benchmarking techniques, datasets, publication strategies, software architectures, and**

emerging scientific approaches can collectively accelerate a foreign adversary's technological development over time. This is particularly true in emerging dual-use fields such as artificial intelligence, semiconductors, aerospace systems, quantum information science, advanced materials, and biotechnology. In these environments, the strategic concern is not solely whether a specific controlled technology is transferred during one isolated collaboration, but whether sustained access to the U.S. research ecosystem incrementally strengthens foreign military or strategic capabilities over time.

Moreover, the United States government routinely recognizes that certain risks are sufficiently high to warrant categorical restrictions rather than case-by-case mitigation. Export controls, sanctions regimes, classified access restrictions, procurement prohibitions, and entity-list designations all reflect the principle that some entities present unacceptable risks due to their conduct, affiliations, or strategic objectives. Research security policy should not be artificially exempted from this broader national security framework. **If the United States Government has already determined that certain entities pose sufficiently serious national security, human rights, military, proliferation, sanctions, or export control concerns to warrant placement on government restricted lists, sanctions lists, or entity lists, it is entirely reasonable to conclude that those same entities should not be permitted to benefit from federally funded research collaborations.**

6. Universities Claim they can Adequately Self-Police

Universities and academic associations frequently argue that institutions are capable of adequately self-policing research security risks without additional statutory safeguards, restrictions, or oversight mechanisms. This argument generally rests on the premise that universities possess sufficient internal compliance structures, ethics policies, disclosure systems, export control offices, and administrative processes to identify and mitigate problematic foreign relationships or malign influence. However, the Select Committee's investigations, along with numerous federal enforcement actions and agency findings over the past several years, demonstrate that this assumption is fundamentally flawed. The research security challenge is not merely a matter of isolated compliance failures; rather, it reflects structural incentive problems embedded throughout the modern research enterprise.

Universities are not neutral actors in this space. Research institutions operate within a highly competitive environment where prestige, grant acquisition, publication output, international partnerships, tuition revenue, and global rankings are heavily incentivized. Faculty members are rewarded for securing larger volumes of federal funding, publishing extensively, expanding international collaborations, and building global research networks. Universities themselves similarly benefit from maximizing indirect cost recovery, increasing sponsored research portfolios, and cultivating international academic relationships. These incentives often directly conflict with the implementation of aggressive research security measures that could slow collaborations, reduce

funding opportunities, increase administrative burdens, or generate reputational concerns. As a result, universities frequently possess institutional incentives to minimize, downplay, or narrowly interpret potential research security risks rather than proactively identify and mitigate them.

As previously discussed, numerous investigations have repeatedly demonstrated that universities often failed to identify undisclosed foreign funding, hidden foreign appointments, talent recruitment program participation, unauthorized parallel research efforts in China, and affiliations with foreign military-linked institutions until those relationships were uncovered externally by federal investigators, federal grant-making agencies, whistleblowers, journalists, or congressional investigators. In many instances, institutions simultaneously certified compliance with federal grant requirements despite lacking meaningful mechanisms to independently verify the accuracy and completeness of faculty disclosures. Put simply, many universities relied heavily on an honor-system model in which institutions accepted faculty representations at face value without conducting robust due diligence, independent validation, or meaningful post-award monitoring.

The argument that universities can self-police also overlooks the asymmetric nature of the threat environment. The Chinese Communist Party's (CCP) MCF strategy explicitly seeks to leverage open research ecosystems, academic collaboration, talent recruitment mechanisms, and international scientific exchanges to advance China's military modernization and strategic technological capabilities. Universities are educational institutions, not counterintelligence or national security organizations, and many lack both the expertise and institutional culture necessary to identify sophisticated foreign influence, concealment tactics, non-transparent funding arrangements, or dual-use technology diversion risks.

Universities' growing financial dependence on foreign gifts, contracts, partnerships, joint institutes, sponsored research arrangements, and overseas funding streams can also create institutional incentives that complicate claims that academia can adequately self-police research security risks. Many major research universities actively compete to attract foreign funding and international partnerships because such relationships provide substantial financial benefits, enhance global rankings, expand research portfolios, increase publication output, and support institutional prestige. These financial relationships can create pressure—whether explicit or implicit—to avoid heightened scrutiny of certain foreign partnerships, minimize reputational damage, preserve funding relationships, or resist safeguards perceived as threatening valuable international collaborations. The issue is not merely whether individual researchers fail to disclose problematic relationships, but whether institutional financial incentives themselves may discourage aggressive oversight, rigorous enforcement, or voluntary disclosure of research security concerns that could jeopardize lucrative foreign relationships or broader institutional interests.

As an example of this dynamic, documents obtained by the Select Committee reveal that the University of Maryland (UMD) hesitated to approve a professor's contract with Huawei before blessing an alternative arrangement. In the correspondence with Huawei, the UMD professor stated, "if you confirm that it is a gift, we may have a chance to move forward."⁶⁴ The Huawei employee responded, "Huawei will be glad to provide gift funding for your research." Ultimately, UMD had approved Huawei research to be provided as a gift rather than a contract despite required outputs. This exchange underscores how universities and researchers often look for semantic workarounds to justify questionable foreign funding rather than establishing and enforcing genuine research security safeguards. UMD and an outside entity conducted an internal investigation that concluded and essentially dismissed the nondisclosure of the funding as a series of unintentional clerical errors.⁶⁵ However, the documents obtained tell a very different story. Correspondence shows that there was awareness of the nature of the Huawei contract and deliberately sought to conceal it by labeling it as a "gift."⁶⁶ This maneuver appears intended to avoid disclosing an active affiliation and research conducted on behalf of Huawei in U.S. government grant documentation. Such actions raise clear conflict-of-interest and conflict-of-commitment concerns and undermine the integrity of federal grant decisions, which rely on full and accurate disclosure to ensure awards are made without foreign influence or competing obligations. In 2024, UMD ultimately settled the case and agreed to pay \$500,000 to resolve allegations that it failed to disclose foreign research support in federal grant proposals.⁶⁷

Moreover, the claim that universities can effectively self-regulate is undermined by the repeated pattern of institutions resisting stronger safeguards until compelled by external pressure. Historically, many universities opposed enhanced disclosure requirements, criticized federal investigative efforts, resisted restrictions on collaborations with high-risk entities, and framed research security concerns as isolated incidents rather than systemic vulnerabilities. In numerous cases, universities only implemented stronger compliance programs after federal investigations, criminal prosecutions, grant suspensions, adverse media exposure, or congressional scrutiny. This reactive posture demonstrates the limitations of relying solely on voluntary institutional self-governance in an area with significant national security implications.

For example, in a Section 117 Foreign Gift and Contracting investigation in 2025 involving Harvard University, the U.S. Department of Education stated that Harvard's foreign funding disclosures contained "incomplete and inaccurate disclosures," including anonymous donors and other deficiencies, despite Harvard previously being investigated for similar issues and subsequently attesting that it had implemented written compliance systems and procedures to ensure adherence with federal disclosure requirements.⁶⁸ The Department further emphasized Harvard's extensive compliance infrastructure, substantial legal resources, and enormous federal funding streams, while nevertheless expressing

concern regarding the university's institutional controls and ability to fully capture and accurately report foreign funding relationships.⁶⁹

In a Section 117 investigation in 2020 involving Stanford University, the U.S. Department of Education raised concerns regarding Stanford's extensive financial and institutional entanglements with the People's Republic of China, including more than \$64 million in anonymous gifts and contracts from China, extensive PRC partnerships, and allegations involving a PLA-affiliated visiting researcher obtaining access to sensitive neurological research activities. The Department further questioned whether Stanford had adequately disclosed foreign funding relationships and noted broader concerns regarding foreign influence, transparency, and the protection of taxpayer-funded research.⁷⁰

The limitations of university self-policing are particularly acute in the context of post-award monitoring. While some institutions have strengthened proposal review and disclosure intake processes, far fewer possess meaningful mechanisms to monitor research activities after federal funding has been awarded. Research collaborations evolve over time. Co-authors change, foreign students and researchers rotate into projects, unpublished know-how is exchanged, datasets move across borders, and new institutional relationships emerge long after the initial grant review process concludes. **Yet most universities—and many federal agencies—still lack scalable systems to continuously monitor publication activity, co-authorship patterns, foreign affiliations, or emerging collaborations involving restricted or military-linked entities.**

Additionally, universities often face inherent reputational conflicts when confronting potential research security violations involving prominent faculty members. Senior researchers frequently generate substantial grant revenue, institutional prestige, industry partnerships, and publication output. Investigating or disciplining such individuals can create financial, reputational, and political costs for institutions. As a result, universities may face strong internal pressures to narrowly construe allegations, avoid public scrutiny, or resolve matters administratively rather than aggressively pursuing accountability. These institutional dynamics further undermine the assumption that universities alone can adequately safeguard taxpayer-funded research from exploitation.

Furthermore, major research universities and academic associations also possess significant political, economic, and institutional influence that can shape congressional and policy debates surrounding research security safeguards.^{71,72} Many large universities are among the largest employers, economic drivers, and recipients of federal funding within their respective congressional districts and states. They often maintain sophisticated government affairs offices, retain lobbying organizations, coordinate through well-funded higher education associations, and engage extensively with Congress and federal agencies to influence legislation, appropriations, regulatory frameworks, and research policy.

In some cases, these efforts are directed toward preserving maximum flexibility over foreign partnerships, limiting restrictions on international collaborations, opposing enhanced compliance obligations, or resisting statutory safeguards that could affect institutional funding streams, research volume, or international engagement. Given the economic and political importance many universities hold within congressional districts, these institutions can exert substantial influence on policymakers and legislative discussions concerning research security. The issue is not that universities should be excluded from policy debates, as they are important stakeholders within the U.S. research ecosystem, but rather that policymakers should recognize the significant institutional incentives, financial interests, and lobbying efforts that may shape academia's opposition to stronger research security protections tied to federally funded research.

Protecting federally funded research requires more than institutional good faith. It requires clear statutory safeguards, enforceable compliance mechanisms, risk-based restrictions and prohibitions, independent oversight, and consistent federal standards capable of addressing systemic vulnerabilities across the research ecosystem.

7. Inconsistent Federal Standards Have Created Confusion and Vulnerabilities Across the Research Ecosystem

Throughout the Select Committee's investigations, universities and university associations have repeatedly argued that the federal government applies inconsistent research security standards across agencies, creating confusion for institutions attempting to navigate compliance obligations. In many respects, this criticism is fair. Different agencies have historically adopted varying definitions, disclosure requirements, risk tolerance thresholds, enforcement mechanisms, prohibited entity frameworks, and compliance expectations. This fragmented approach has created gaps, inconsistencies, and ambiguity within the research ecosystem.

At the same time, institutions cannot use the existence of inconsistent federal standards as a blanket justification for failing to address obvious research security risks, ignoring clear warning signs, or resisting reasonable safeguards. Many of the vulnerabilities identified over the years involved conduct or relationships that raised serious concerns regardless of which agency framework applied. Nevertheless, the absence of a centralized and uniform government-wide framework has contributed to uncertainty across the research ecosystem and complicated compliance efforts for universities, federal agencies, and researchers alike.

Importantly, the Select Committee's recommendations throughout its investigations have remained consistent. The Committee has repeatedly advocated for clear, standardized, risk-based safeguards that establish uniform baseline protections across federally funded research programs. To address the very concerns universities and associations have raised, the Select Committee developed the Securing Innovation and Research from Adversaries (SIRA) Act

(H.R. 8901).⁷³ SIRA is designed to establish a government-wide baseline prohibition framework for federally funded research collaborations involving foreign entities and persons appearing on U.S. government restricted or entity lists. The purpose of the legislation is to eliminate ambiguity, reduce inconsistent interpretations across agencies, and provide a clear statutory standard that applies uniformly throughout the federal research enterprise.

SECTION III: INSTITUTIONAL DEFENSE AND PUSHBACK

8. “By Adding Requirements and Prohibiting Certain Collaborations on Federally Funded Research, the Federal Government Is Infringing on Academic Freedom”

Opponents of enhanced research security safeguards frequently argue that imposing restrictions, compliance requirements, or prohibitions on certain foreign collaborations infringes upon academic freedom. This argument fundamentally mischaracterizes both the nature of academic freedom and the federal government’s longstanding authority to establish conditions governing the use of taxpayer-funded research awards. **Academic freedom does not create an unrestricted entitlement to receive federal funds free from oversight, accountability, or safeguards.** Nor does it require the United States government to subsidize collaborations that present unacceptable risks to U.S. national security, technological leadership, or taxpayer interests.

Participation in federally funded research is voluntary. Universities and researchers are free to pursue research independently, collaborate internationally, publish openly, and engage with foreign institutions using private funding or institutional resources, subject to applicable law. What is at issue is not whether academic inquiry may occur, but whether the federal government is obligated to finance, facilitate, or support particular activities using taxpayer dollars. Congress has both the constitutional authority and affirmative responsibility to ensure that federal funds are spent in a manner consistent with the national interest. This necessarily includes establishing reasonable and commonsense safeguards to prevent taxpayer-funded research from being exploited by foreign adversaries, diverted to military end uses, or used to advance the strategic objectives of hostile foreign governments. Moreover, federal agencies themselves can take proactive measures by updating award terms and conditions, implementing enhanced compliance requirements, and establishing clear prohibitions governing the use of federally funded research awards.

Additionally, universities are not limited to merely complying with minimum federal requirements. They could take proactive measures to reduce risk, including prohibiting research relationships with entities that appear on U.S. government restricted lists, sanctions lists, export control lists, or other government-designated entity lists. Such actions would demonstrate a genuine and proactive commitment to protecting taxpayer-funded research and ensuring that university research activities do not inadvertently benefit foreign adversaries

or entities that the U.S. government has already identified as posing national security, human rights, or proliferation concerns.

Federal research awards have typically never existed without conditions. Universities already comply with federal requirements tied to grants and contracts, including regulations involving export controls, cybersecurity, research misconduct, human subject protections, animal research protocols, financial auditing, conflicts of interest, nondiscrimination, classified information handling, controlled unclassified information, procurement integrity, and disclosure obligations. Academic institutions routinely accept these conditions as part of receiving federal funding. Research security safeguards are no different. The argument that restrictions become impermissible only when they concern collaborations involving foreign adversaries or high-risk entities reflects a selective and inconsistent understanding of federal grant-making authority.

Moreover, the modern research environment differs dramatically from the geopolitical and technological landscape that existed when many traditional assumptions surrounding academic openness were formed (see NSDD-189 section later in this report). Today, the CCP actively pursues a strategy of MCF designed to systematically leverage civilian research ecosystems, academic collaboration, talent recruitment, and scientific exchange to accelerate China's military modernization and strategic technological development. Under this framework, ostensibly civilian universities, laboratories, and companies may directly support the PLA, Chinese defense-industrial entities, state surveillance programs, or other strategic national objectives. In this environment, the federal government cannot responsibly ignore the downstream national security implications associated with federally funded research collaborations.

The invocation of academic freedom also frequently obscures the distinction between restricting ideas and regulating the expenditure of federal funds. Research security measures generally do not prohibit scholars from discussing ideas, publishing research, teaching students, or engaging in lawful academic inquiry. Rather, they establish conditions governing how federal taxpayer dollars may be used. Congress routinely attaches conditions to federal spending programs to ensure funds advance legitimate governmental interests. Preventing federally funded research from benefiting foreign military-linked entities, sanctioned organizations, or state-directed technology acquisition efforts is plainly within the scope of those interests.

Additionally, these arguments often ignore the federal government's obligation to serve as a responsible steward of taxpayer resources. Federal research funding is not charity, nor is it an unconditional entitlement owed to universities. Taxpayer-funded research programs exist to advance the interests, security, prosperity, and technological leadership of the United States. **The American public has a legitimate expectation that billions of dollars in federally funded research will not be used, directly or indirectly, to strengthen the military, intelligence, surveillance, or strategic capabilities of foreign adversaries.** Congress would be

failing in its constitutional responsibilities if it knowingly appropriated funds without implementing safeguards designed to mitigate those risks.

9. “Enacting Restrictions will Harm Innovation”

Opponents of enhanced research security measures frequently argue that imposing restrictions on certain foreign collaborations, disclosure requirements, named entity prohibitions, or compliance safeguards will harm innovation and undermine the openness that has historically contributed to the success of the U.S. research enterprise. While openness and scientific exchange have undeniably played an important role in American innovation, this argument presents a false choice between innovation and security. In reality, long-term innovation leadership depends not only on openness, but also on the protection, integrity, and strategic stewardship of the very research ecosystem the United States has spent decades and billions of taxpayer dollars building.

Historically, the United States achieved some of its greatest periods of scientific and technological advancement while simultaneously maintaining robust national security safeguards and technology protection measures. During the Cold War, the United States led the world in aerospace, computing, semiconductors, nuclear science, telecommunications, and defense technologies despite extensive export controls, classified research programs, restrictions on sensitive technology transfers, and strategic limitations on adversarial access to advanced research. The existence of targeted safeguards did not prevent innovation; rather, those safeguards helped preserve the United States’ technological advantage during periods of intense geopolitical competition. The notion that innovation can only flourish in the complete absence of restrictions is contradicted by decades of American scientific and industrial history.

The argument also incorrectly assumes that all international collaboration produces equal benefits while carrying equal risks. It ignores the reality that strategic competitors such as the PRC actively pursue state-directed technology acquisition strategies designed to leverage open research ecosystems for military, economic, and geopolitical advantage. Under China’s MCF strategy, advances originating in civilian academic environments may directly support the modernization of the PLA, surveillance systems, advanced weapons development, cyber capabilities, or strategic industrial policies. In such an environment, unrestricted access to cutting-edge U.S. research can accelerate the erosion of America’s own technological leadership. Failing to impose reasonable safeguards does not protect innovation; it risks subsidizing the transfer of innovation to strategic competitors using American taxpayer dollars.

Moreover, the long-term consequences of inadequate research security can severely stunt innovation. When federally funded research is diverted, exploited, or replicated abroad through non-transparent collaborations or state-backed technology acquisition efforts, the United States risks losing the very competitive advantages that sustain its innovation ecosystem. The loss of technological

leadership in critical sectors such as artificial intelligence, semiconductors, quantum information science, biotechnology, aerospace, and advanced manufacturing would carry profound economic and national security consequences. **Protecting strategic research advantages is therefore not contrary to innovation policy; it is essential to preserving America’s future capacity to innovate.**

Additionally, many critics of research security measures apply standards to the United States that strategic competitors themselves do not follow. China heavily restricts foreign access to sensitive research areas, limits external participation in strategic technologies, closely integrates state priorities into research planning, and aggressively protects technologies deemed important to national development and military modernization. The expectation that the United States should maintain completely unrestricted openness while strategic competitors operate under far more controlled and state-directed systems creates an asymmetric vulnerability that disadvantages American researchers, institutions, and taxpayers.

The innovation argument also frequently overlooks the role of public trust in sustaining federal research investment. **The American public is more likely to support robust federal funding for scientific research when there is confidence that taxpayer dollars are being protected from exploitation, diversion, fraud, and misuse.** Persistent revelations involving undisclosed foreign ties, hidden affiliations, talent recruitment programs, unauthorized technology transfer, or collaborations with military-linked entities risk undermining public and congressional support for federally funded research programs. Reasonable safeguards can therefore strengthen, rather than weaken, the long-term sustainability of the U.S. research enterprise by reinforcing accountability and public confidence.

Ultimately, innovation and research security are not mutually exclusive objectives. A secure research ecosystem is a durable research ecosystem. Protecting federally funded research from exploitation by foreign adversaries helps preserve the scientific, economic, and strategic advantages that allow the United States to remain the world’s leading center of innovation. The question is not whether openness has value—it unquestionably does. The question is whether the United States should continue subsidizing activities that may accelerate the erosion of its own technological leadership. Reasonable, risk-based safeguards are not obstacles to innovation; they are necessary measures to ensure that American innovation continues to benefit the United States rather than strategically empowering its adversaries.

10. “Research Security Requirements Create an Undue Administrative Burden on Universities and Faculty”

Universities and academic associations frequently argue that enhanced research security safeguards, disclosure requirements, compliance reviews, and restrictions

on high-risk collaborations impose an undue administrative burden on research institutions. While compliance obligations do require effort and resources, this argument often reflects an expectation that universities should continue receiving billions of dollars in taxpayer-funded research awards without implementing the level of oversight, due diligence, and accountability reasonably expected in virtually every other federally funded or regulated sector. The position is particularly difficult to reconcile given the enormous scale of federal funding many institutions receive and the strategic national security implications associated with that research.

Federal research funding is not an unconditional subsidy or entitlement issued without responsibilities. Many universities receive hundreds of millions—and in some cases billions—of dollars annually through federal grants, contracts, cooperative agreements, and other research awards funded by American taxpayers. Those funds support advanced research in areas directly tied to U.S. economic competitiveness, military superiority, critical infrastructure, emerging technologies, public health, and national security. With that level of public investment necessarily comes an obligation to implement appropriate compliance systems, internal controls, risk management practices, and oversight mechanisms designed to protect those funds from fraud, abuse, diversion, and foreign exploitation. It is neither unreasonable nor extraordinary for the federal government to expect institutions receiving substantial taxpayer support to maintain robust safeguards and due diligence commensurate with the risks involved.

Universities already comply with extensive administrative requirements in countless other areas whenever institutional interests, accreditation standards, liability concerns, or federal funding conditions are implicated. Academic institutions maintain sophisticated bureaucracies dedicated to financial auditing, Title IX compliance, export controls, human subjects protections, animal research oversight, environmental health and safety, cybersecurity compliance, procurement regulations, conflict-of-interest disclosures, accreditation standards, and intellectual property management. Universities routinely expand administrative infrastructure when required to preserve funding streams, avoid liability, or maintain regulatory standing. The claim that research security requirements are uniquely unmanageable therefore appears less rooted in actual institutional incapacity and more reflective of resistance to additional scrutiny, oversight, and accountability in an area that may complicate international partnerships or slow the pace of grant administration.

Many of the safeguards characterized as “burdensome” represent basic due diligence measures that would be considered standard risk management practices in other sectors handling sensitive information, critical technologies, or significant federal funding. Verifying foreign affiliations, screening collaborators against government entity lists, monitoring conflicts of interest and commitment, tracking federally funded publications, conducting post-award compliance reviews, or

requiring accurate disclosures are not extraordinary expectations given the strategic value of the research involved.

The “undue burden” argument also frequently ignores the costs imposed on the United States when adequate safeguards are absent. Over the past decade, federal investigations have repeatedly uncovered undisclosed foreign funding, hidden foreign appointments, talent recruitment program participation, unauthorized technology transfer, research misconduct, grant fraud, and collaborations involving entities linked to foreign militaries or strategic competitors. These failures impose substantial national security, economic, and reputational costs on the United States. The burden associated with implementing preventative safeguards must be weighed against the far greater consequences of allowing taxpayer-funded research to be systematically exploited by foreign adversaries operating sophisticated state-directed technology acquisition efforts.

Additionally, technological solutions already exist that significantly reduce many of the claimed compliance burdens. Publication databases, bibliometric tools, entity-list matching software, automated disclosure systems, ORCID integration, grant management platforms, and data analytics capabilities can substantially streamline monitoring and risk identification processes. Many institutions already use sophisticated research administration systems capable of managing large-scale compliance operations. Assertions that universities are incapable of implementing meaningful research security oversight often underestimate both the administrative capacity of major research institutions and the degree to which existing compliance infrastructure can be adapted to incorporate research security functions.

Importantly, the federal government is not obligated to subordinate national security or ethical concerns to institutional convenience. The fact that compliance requirements may require additional staffing, training, vetting, monitoring, or administrative review does not render those safeguards inappropriate or excessive. Universities voluntarily choose to compete for and accept federal awards because those awards provide substantial financial, reputational, and institutional benefits. Acceptance of federal funding necessarily carries obligations. Institutions cannot reasonably demand access to billions of dollars in taxpayer-funded research support while simultaneously objecting to the implementation of safeguards designed to ensure those funds are not misused, diverted, or exploited by foreign adversaries.

Furthermore, Congress and the Executive Branch have both the authority and the responsibility to establish conditions on the expenditure of taxpayer-funded research awards. Federal research grants are not entitlements. They are discretionary awards funded by American taxpayers and issued subject to terms, conditions, certifications, reporting requirements, and compliance obligations deemed necessary to protect the public interest. Universities, principal investigators, and research institutions routinely accept extensive administrative, financial, ethics, export control, human subjects, cybersecurity, and reporting

requirements as a condition of receiving federal funding. Put simply, recipients seeking access to federal research funding do not have a right to taxpayer dollars on their preferred terms. The United States Government has every right to determine how its funds are spent, what conditions accompany those funds, and which foreign entities are inappropriate partners for research conducted with taxpayer support.

Universities and principal investigators remain free to decide whether they wish to accept federal research funding. Participation in federal grant programs is voluntary, not mandatory. If an institution is unwilling to complete additional certifications, provide enhanced disclosures, conduct reasonable due diligence, participate in research security training, or comply with restrictions involving entities that the United States Government has already identified as posing national security, sanctions, export control, or other risks, it may choose not to apply for or accept the award. What it cannot reasonably demand is unrestricted access to taxpayer funding while objecting to the safeguards that Congress and federal agencies determine are necessary to protect that funding from misuse or exploitation.

11. “Many Research Security Issues Only Amount to Clerical or Paperwork Mistakes”

A common argument advanced by portions of academia is that many research security violations amount to nothing more than inadvertent clerical mistakes, administrative oversights, or confusing paperwork errors rather than substantive misconduct warranting heightened concern or enforcement action. While isolated administrative mistakes can and do occur in any large compliance system, this argument significantly understates both the seriousness and recurring nature of many research security violations identified by federal agencies, law enforcement, inspectors general, and congressional investigations over the past decade.

The NSF suspension and debarment records examined in this report illustrate the distinction between an isolated paperwork mistake and a substantive compliance failure. Across multiple matters, federal investigators identified undisclosed foreign positions, foreign compensation, outside research support, talent program participation, conflicts of commitment, inaccurate certifications, and other relationships that were directly relevant to federal award requirements. In some cases, the omitted relationships persisted for years, involved formal appointments or contractual obligations, and appeared across multiple proposals, awards, or agency disclosure processes. NSF OIG did not evaluate these matters merely by asking whether a form had been completed incorrectly; it examined the underlying facts, the materiality and duration of the omitted relationships, the researcher’s disclosure obligations, and whether the conduct called into question the individual’s present responsibility to receive federal funds.

First, the repeated pattern of undisclosed foreign funding, hidden appointments, unreported affiliations, concealed participation in foreign talent recruitment

programs, false certifications, and misleading grant disclosures cannot reasonably be dismissed wholesale as harmless paperwork mistakes. In many investigated cases, the omissions involved extensive foreign relationships spanning years, significant compensation arrangements, formal contractual obligations, overseas laboratory appointments, foreign government funding streams, recruitment agreements, or parallel research activities conducted abroad. These were not isolated typographical errors or accidental omissions buried in administrative forms. Rather, many involved substantive foreign relationships directly relevant to federal grant eligibility, conflict-of-interest determinations, and national security risk assessments.

Second, the “clerical error” argument ignores the reality that disclosure and certification systems exist precisely because the underlying information is materially important to the federal government’s funding decisions. If foreign affiliations, outside funding, foreign government contracts, talent recruitment participation, or institutional ties were insignificant, federal agencies would not require researchers and institutions to disclose them as conditions of receiving taxpayer-funded awards. These requirements exist because such information bears directly on issues involving conflicts of interest, conflicts of commitment, intellectual property risks, undue foreign influence, research integrity, and national security vulnerabilities. Dismissing failures to provide that information as mere paperwork problems trivializes the very purpose of the disclosure system itself.

Moreover, many federal awards require certifications made under penalty of law or subject to administrative enforcement mechanisms. Universities and principal investigators routinely certify that disclosures are accurate, complete, and compliant with agency requirements. The integrity of the federal research funding system depends heavily on the accuracy of those certifications. If institutions and researchers are permitted to characterize major omissions as inconsequential clerical mistakes whenever problematic relationships are discovered, the disclosure and compliance framework becomes effectively meaningless. Compliance systems cannot function if material inaccuracies are routinely excused after the fact as administrative misunderstandings.

The “paperwork error” defense is also difficult to reconcile with the increasingly sophisticated compliance infrastructures maintained by major research universities. Many institutions possess extensive research administration offices staffed by compliance professionals, attorneys, export control specialists, grant managers, and disclosure personnel whose purpose is to assist faculty in navigating federal requirements. Universities routinely require mandatory trainings, annual disclosure updates, conflict-of-interest certifications, and grant compliance reviews. In many cases, faculty members receive repeated instructions regarding disclosure obligations and institutional reporting requirements. Against this backdrop, claims that recurring nondisclosures involving substantial foreign relationships are merely accidental administrative oversights become less

persuasive, particularly where the omitted relationships involve formal contracts, overseas employment, foreign compensation, or sustained participation in foreign government-sponsored programs.

Importantly, even where a violation does originate as negligence or recklessness rather than deliberate concealment, the consequences can still be serious. Research security risks do not disappear simply because an omission was characterized as unintentional. An undisclosed foreign affiliation involving a military-linked institution, a sanctioned entity, or a foreign government-backed talent program may still expose federally funded research to exploitation, unauthorized technology transfer, or conflicts of interest regardless of whether the reporting failure was intentional or negligent. Federal compliance systems routinely impose consequences for reckless or negligent failures because the integrity of federally funded programs depends on accurate reporting and responsible stewardship of taxpayer resources.

Additionally, the repeated invocation of “clerical errors” risks obscuring a broader systemic issue within portions of the academic research enterprise: namely, that for many years research security compliance was often treated as a secondary administrative concern rather than a serious national security responsibility. Some institutions prioritized maximizing research volume, accelerating grant acquisition, and expanding international partnerships while devoting comparatively limited attention to verifying disclosures, monitoring foreign affiliations, or assessing strategic technology transfer risks. The resulting compliance culture sometimes fostered an environment in which disclosure obligations were viewed as bureaucratic formalities to complete rather than substantive safeguards designed to protect taxpayer-funded research from exploitation.

The federal government would never accept similar arguments in many other regulated sectors receiving substantial public funds. Defense contractors, financial institutions, healthcare providers, and entities handling classified or export-controlled information are expected to maintain rigorous compliance systems, accurate certifications, and internal controls. Significant omissions involving foreign relationships, financial interests, or regulatory disclosures in those sectors would not simply be dismissed as harmless paperwork errors. Universities receiving billions of dollars in taxpayer-funded research support should not be held to a lower standard.

Ultimately, while genuine administrative mistakes may occur in isolated circumstances, the persistent pattern of undisclosed foreign relationships and research security-related compliance failures identified across the research enterprise demonstrates that the issue extends far beyond mere clerical error. The integrity of federally funded research depends on accurate disclosures, meaningful oversight, and institutional accountability. Characterizing substantive omissions and compliance failures as insignificant paperwork mistakes minimizes

serious vulnerabilities that carry substantial national security, economic, and strategic implications for the United States.

The following four cases from the NSF OIG records underscore the serious nature of compliance failures and violations.

A 2025 NSF OIG's debarment recommendation involving former NSF Program Officer and University of Florida professor Dr. Tao Li demonstrates that research security and research integrity failures can have profound real-world consequences extending far beyond administrative noncompliance or purported "clerical errors." The investigation uncovered undisclosed affiliations with PRC-linked programs, duplicate foreign-funded proposals submitted to NSF, abuse of his position as an NSF Program Officer in an alleged quid pro quo arrangement, falsified research results, destruction of evidence, and repeated lack of candor during multiple investigations. Most damningly, the investigation found that Li knowingly and intentionally fabricated research results in a paper linked to the suicide of his graduate student and mentee, who accused Li in his suicide note of forcing him to falsify data and expressed fear that exposing the misconduct would ruin both of their reputations. The case resulted in a 15-year ban by the Association for Computing Machinery (ACM), retraction of the falsified publication, multiple NSF award terminations, and a recommendation for government-wide debarment.⁷⁴

In a 2022 NSF suspension and debarment matter involving Dr. Mingqing Xiao of Southern Illinois University-Carbondale, the conduct extended far beyond a mere clerical or paperwork issue. NSF OIG alleged that Dr. Xiao intentionally omitted required foreign support information from Current and Pending Support disclosures submitted to NSF in order to improve the likelihood of receiving a federal award. The matter also involved a separate NSF research misconduct finding for plagiarism, where NSF concluded that Dr. Xiao copied material into NSF proposals in violation of federal research misconduct standards. In addition, Dr. Xiao was criminally indicted on multiple charges, including wire fraud, false statements, false statements on tax returns, and failure to report foreign bank accounts. Dr. Xiao was convicted on multiple counts involving false tax statements and failure to disclose foreign financial accounts.⁷⁵ NSF OIG ultimately recommended debarment on the grounds that his conduct demonstrated a lack of present responsibility necessary to safeguard federal funds. This fact pattern illustrates that these cases frequently involve substantive misconduct, intentional concealment, false certifications, research integrity violations, and criminal conduct, not harmless administrative mistakes or insignificant paperwork errors.

In a separate NSF suspension matter involving Stanford University, NSF OIG determined that the issues at hand extended far beyond isolated clerical or paperwork mistakes. As part of a proactive investigation into foreign funding disclosures, NSF OIG identified at least 26 NSF awards involving Stanford-affiliated researchers who were simultaneously participating in foreign-funded research projects that were not disclosed to NSF as required. According to NSF

OIG, the undisclosed foreign-funded projects were tied to more than \$12.8 million in claimed award costs, with numerous NSF awards still active at the time of the investigation. The matter involved multiple principal investigators and co-principal investigators across a broad range of federally funded scientific research areas, including artificial intelligence, robotics, engineering, materials science, biotechnology, and autonomous systems. NSF OIG further noted that Stanford's own Senior Director of Pre-Award Operations acknowledged that the university did not independently verify the accuracy of disclosures submitted by principal investigators and instead relied almost entirely on faculty self-reporting. The investigation also identified a Stanford principal investigator who allegedly held a Thousand Talents Program position requiring work at a foreign university for several months per year that had not been disclosed to NSF despite Stanford reportedly being aware of the position for years. NSF OIG ultimately concluded that the failures involved systemic disclosure deficiencies, repeated nondisclosures of foreign funding and affiliations, potential overcommitment concerns, and broader institutional oversight failures serious enough to warrant recommendations to suspend multiple active NSF awards while the investigation continued.

In a 2020 NSF suspension matter involving Dr. Enrique Lavernia, then-Provost and Executive Vice Chancellor of the University of California-Irvine, NSF OIG determined that the conduct at issue extended far beyond simple paperwork or clerical mistakes. NSF OIG substantiated that Lavernia repeatedly failed over many years to disclose extensive foreign affiliations, foreign funding, and formal positions tied to entities in the People's Republic of China while simultaneously receiving millions of dollars in federal funding from NSF, NASA, and DOE. The investigation substantiated that Lavernia held positions including strategic scientist at Wuhan University of Technology, dean of an international materials science institute in China, honorary professor appointments, and participation in China's Thousand Talents Program, while also receiving associated compensation and foreign research support that were not disclosed in federal proposals as required. NSF OIG further identified that Lavernia omitted these relationships in connection with a DOE Top Secret clearance reinvestigation and failed to disclose relevant China affiliations tied to NASA awards subject to statutory China collaboration restrictions. The matter also involved evidence that Lavernia participated in PRC government-backed programs designed to support China's scientific, industrial, and defense modernization efforts, including work tied to advanced materials and additive manufacturing technologies with stated military and national defense applications.⁷⁶ NSF OIG concluded that Lavernia's conduct demonstrated a longstanding pattern of deception, repeated false statements and omissions, disregard for federal disclosure requirements, and conduct serious enough to warrant a recommendation for governmentwide suspension to protect the public interest and prevent further access to federal funds during the ongoing investigation. Additionally, Dr. Lavernia personally received a document from the Chinese Academy of Engineering describing his contributions as a participant in

the Thousand Talents Program. The document credited his work with “**leading China to develop new materials and technologies for cutting-edge defense weapons and equipment, such as nanomaterial synthesis, multiscale fine structure control, and additive manufacturing technology, and continuously narrowing the technology gap with more advanced countries.**” This acknowledgment is particularly significant because it comes from a Chinese government organ and directly links the expertise and research associated with Dr. Lavernia's activities to China's efforts to advance technologies with clear defense and military applications.

Figure 13 – Chinese Academy of Engineering Document Detailing a 12-Year Research Partnership with Dr. Enrique Lavernia Outlining Contributions to Chinese Weapons and Equipment Development

与武汉理工大学建立合作的12年来，Enrique Lavernia教授围绕轻质高强、结构—功能一体化先进复合材料领域中重大科学问题与工程化应用，与我校材料学科首席教授张联盟教授团队开展合作，在高熵合金、非晶混熔与薄带成型，多相、多尺度铝基和氧化锆基复合材料及其制备技术等方面取得了重要进展，初步建立了装备条件国际一流的联合实验室和联合研究团队，联合发表了一批高水平论文，引进和培养了一批优秀人才。

一、引领我国面向国防尖端武器装备的新材料与技术，如纳米材料合成、多尺度精细结构调控、增材制造技术等，不断缩小国内外技术差距

12. “NSDD-189 Requires Fundamental Research to Remain Open and Unrestricted to the Maximum Extent Possible”

NSDD-189 is frequently cited as a basis for opposing expanded research security safeguards and restrictions on federally funded research collaborations. Issued in 1985 during the Reagan Administration, National Security Decision Directive 189 established a policy preference that, to the maximum extent possible, the products of fundamental research should remain unrestricted and that classification should serve as the primary mechanism for controlling sensitive information generated through federally funded research.⁷⁷ At the time, NSDD-189 reflected the geopolitical realities, technological environment, and research ecosystem of the mid-1980s. However, the global research landscape and the nature of strategic technology competition have changed dramatically in the four decades since the directive was issued.

NSDD-189 was never intended to create an unrestricted research environment entirely free from national security safeguards, oversight, or limitations on federally funded research relationships. Even at the time NSDD-189 was issued,

the United States maintained export controls, classification authorities, sanctions regimes, restricted technologies, foreign ownership restrictions, and numerous other national security protections governing sensitive research and technology transfer.

Nothing in NSDD-189 prohibits the federal government from imposing conditions on the use of taxpayer-funded research awards, restricting collaborations involving foreign adversaries, or implementing safeguards necessary to protect U.S. national security interests. Nor does NSDD-189 create an entitlement for universities or researchers to receive unrestricted federal funding regardless of the nature of the foreign entities involved or the strategic implications of the collaboration.

The threat environment confronting the United States today differs fundamentally from the environment that existed when NSDD-189 was developed in 1985. The directive predates the Chinese Communist Party's modern military-civil fusion strategy, large-scale state-directed technology acquisition efforts, systematic foreign talent recruitment programs, cloud-based research collaboration, advanced artificial intelligence ecosystems, quantum information science competition, and the highly globalized academic research networks that now exist. It also predates the extraordinary scale of China's integration into the U.S. research enterprise and the extensive evidence accumulated over the past decade demonstrating how foreign adversaries can exploit open research environments, undisclosed affiliations, joint laboratories, talent programs, and collaborative research relationships to accelerate military and strategic objectives.

A policy framework developed nearly forty years ago should not be treated as immutable despite profound changes in the geopolitical, technological, and research security landscape. Updating how the federal government interprets and operationalizes research security protections does not undermine the core principle that openness can benefit scientific advancement. Rather, it reflects the reality that openness without appropriate safeguards can also create vulnerabilities that foreign adversaries actively exploit.

Applying modern research security safeguards to federally funded research is entirely consistent with the broader purpose of protecting the U.S. research enterprise and ensuring that taxpayer-funded innovation advances American interests rather than directly or indirectly supporting the military modernization or strategic objectives of foreign adversaries. NSDD-189 should therefore be understood within its historical context and updated to reflect the realities of today's research security environment.

SECTION IV: CLAIMS OF XENOPHOBIA

13. Claims of Xenophobia and Allegations of Targeting Ethnic and Ethnically Connected Chinese Researchers

The claim that research security and law enforcement efforts are driven by xenophobia or target individuals based on ethnicity mischaracterizes both the

intent and the evidentiary basis of these concerns. The focus is not on race, nationality, or background. It is on documented behaviors, institutional affiliations, and malign activities that create risk to U.S. research and national security. The United States has long benefited from the contributions of Chinese American researchers, and that remains true. The issue at hand is not who someone is, but what they are doing, who they are working with, and whether those activities implicate legal, policy, or security concerns.

Critically, this argument cannot ignore the Chinese government's own publicly stated policies and directives. Chinese laws, policy documents, and official programs explicitly call for the mobilization of global talent, including individuals of Chinese descent overseas, to support national strategic objectives, including technology acquisition and military-civil fusion. They are outlined in publicly available statutes, talent program agreements, and government strategies that "encourage technology transfer from ethnic Chinese scholars overseas,"⁷⁸ transfer of knowledge, research outputs, and expertise back to China. In some cases, these programs include contractual obligations tied to intellectual property, co-authorship, or the establishment of research ties with Chinese institutions, including those linked to the defense ecosystem.

Yet, notably absent from this debate is any meaningful acknowledgment or criticism of China's policies targeting individuals of Chinese descent abroad by the same universities and academic associations that are quick to label U.S. research security efforts as discriminatory. There is little to no public condemnation by universities, university associations, or advocacy groups like the Committee of 100 of the Chinese government explicitly targeting individuals based on ethnicity to advance state-directed strategic objectives.

Institutions that claim to champion academic integrity, transparency, and non-discrimination have largely avoided confronting the implications of China's policies (while they simultaneously take foreign gifts and contracts from China and partner with foreign entities of concern), even as they directly shape the risk environment within which U.S. research operates. It raises a fundamental question: why is there significant scrutiny of U.S. efforts to address documented risks, but little to no scrutiny of the foreign policies and practices that actively seek to exploit those very systems? Why are universities, university associations, or organizations not taking a more active role in protecting Chinese students and nationals, and Chinese Americans from exploitation by the Chinese government?

By ignoring or downplaying the role of these foreign government policies, the conversation is reframed away from conduct and risk and toward identity-based narratives that obscure the underlying issue. Addressing research security risks is not about targeting individuals. It is about responding to a strategic environment that is openly defined by foreign governments themselves. If institutions are serious about the principles they espouse, they must be willing to confront both sides of that equation, not just the one that is politically convenient.

Recommendations

Although this report focuses on assessing common arguments used to oppose strengthened research security safeguards, detailing recommendations for action remains necessary because these narratives directly shape policy decisions, institutional behavior, agency implementation, and public understanding of research security threats. Many of the arguments examined throughout this report are routinely used to resist or weaken reasonable safeguards designed to protect federally funded research from exploitation by foreign adversaries. Accordingly, it is not sufficient to merely identify flaws in these claims. The Select Committee believes it is equally important to recommend concrete policy, oversight, and compliance measures capable of addressing the underlying vulnerabilities, institutional incentives, and systemic weaknesses discussed throughout this assessment.

1. Pass the Securing Innovation and Research from Adversaries (SIRA) Act

The SIRA Act would prohibit any individual, while participating in or performing work under a federally funded research award, from conducting research with any entity, or any individual affiliated with an entity, on a United States Government restricted entity list.^b The Committee recommends prohibiting federally funded research collaboration with any entity or individual affiliated with an entity listed on a U.S. government restricted entity list. This prohibition should apply regardless of whether the collaboration is bilateral or occurs through multilateral engagements, including coauthored publications that fall outside the narrow category of “hyper-authored” research. This approach builds on the Department of War’s updated risk matrix, which now restricts such collaboration.⁷⁹ By closing gaps that allow indirect or distributed collaboration with entity listed entities, this policy would strengthen research security, ensure compliance with existing restrictions, and prevent federally funded research from supporting entities designated as national security risks. **Universities do not need to wait for additional federal policy or for Congress to enact the SIRA Act before adopting stronger research security safeguards. Institutions can proactively implement this commonsense approach by establishing their own policies prohibiting federally funded research collaborations with entities that pose identified national security risks.**

^b “Restricted entity list” refers collectively to United States government lists identifying foreign individuals, companies, universities, laboratories, or organizations subject to sanctions, export controls, procurement restrictions, or other national security-related prohibitions or limitations. These lists include, but are not limited to, the Department of Commerce Bureau of Industry and Security (BIS) Entity List, the Department of Defense lists established under Sections 1260H and 1286 of the National Defense Authorization Act (NDAA), the Department of the Treasury Office of Foreign Assets Control (OFAC) sanctions lists, and the Uyghur Forced Labor Prevention Act (UFLPA) Entity List. Inclusion on such lists generally reflects U.S. government determinations related to national security, military end use or end users, human rights abuses, sanctions evasion, or other activities contrary to the national security or foreign policy interests of the United States.

2. Standardized Author Contribution Disclosure Requirements for (at a minimum) Federally Funded Research

Federal agencies should require standardized author contribution statements for publications, preprints, conference papers, and other outputs resulting from federally funded research. At a minimum, disclosures should identify each author's role in conceptualization, methodology, experimentation, data collection, analysis, software, funding, supervision, writing, and project administration. Recipient institutions should certify the accuracy of these statements and retain them as part of the research record. Additionally, federal agencies should evaluate whether knowingly inaccurate or misleading author contribution disclosures tied to federally funded research constitute research misconduct, false certification, or other compliance violations warranting administrative action, including suspension, debarment, or funding restrictions where appropriate.

3. Create Incentives for Universities That Adopt Strong Research Security Practices

The federal government should consider establishing incentives for institutions that voluntarily and proactively adopt robust research security practices that exceed minimum federal requirements. Universities that implement meaningful safeguards (such as the SIRA Act list-based prohibitions), conduct enhanced due diligence, prohibit research collaborations with high-risk entities, and demonstrate a sustained commitment to protecting federally funded research could be designated as **"trusted universities"** for research security purposes.

The federal government could pair such a designation with tangible incentives, including giving qualifying institutions additional consideration or priority, where permitted by law and consistent with merit-based review, for certain federal research funding opportunities. Universities that proactively strengthen their research security programs should have an opportunity to benefit from doing so rather than viewing enhanced safeguards solely as an additional compliance burden.

This approach could create a reinforcing cycle of benefits. Increased federal research funding could enable participating universities to expand laboratories, research programs, infrastructure, and faculty positions; attract additional researchers seeking well-funded and secure research environments; and strengthen their ability to compete for future federal awards. For emerging research institutions, including R2 universities seeking to expand their research enterprise and potentially attain R1 status, increased research activity and investment could contribute to broader institutional growth and research capacity.

These incentives could also encourage other universities to adopt comparable safeguards as they observe federal research investment flowing toward institutions that have proactively demonstrated strong research security practices.

Over time, this could create a broader institutional incentive to compete not only on research excellence, but also on the ability to protect federally funded research.

The result could be a positive domino effect: stronger research security practices lead to greater confidence in participating institutions, which can support additional research investment, attract researchers and faculty, expand laboratory capacity, and further strengthen the U.S. research enterprise. At the same time, these safeguards would help protect American human and intellectual capital from being diverted to foreign entities that present national security risks.

4. Government-Wide Adoption of Fact-Based Suspension and Debarment Authorities Beyond Conviction-Based Suspension and Debarments

Federal agencies should standardize use of fact-based suspension and debarment authorities to address research security violations, false certifications, undisclosed foreign affiliations, and noncompliance with award terms. Agencies should not treat criminal convictions, civil judgments, or prosecution as prerequisites for administrative accountability. Suspension and debarment are protective remedies designed to safeguard federal funds and assess present responsibility.

Prosecutors may decline criminal or civil cases for reasons unrelated to the underlying conduct, including evidentiary issues, competing priorities, resource constraints, jurisdictional concerns, or monetary thresholds. Such declinations do not establish that no award, disclosure, or compliance violation occurred.

Agencies should therefore act on credible investigative findings, inspector general reports, institutional records, admissions, audit findings, and false certifications, and should apply administrative remedies where appropriate to individual researchers, institutions, and affiliated entities. Agencies should also more aggressively use available administrative false claims authorities to address materially false certifications, undisclosed conflicts, and other misrepresentations tied to federal research funding.

Endnotes

¹ U.S. Department of Education, Office of the General Counsel, Institutional Compliance with Section 117 of the Higher Education Act of 1965, October 2020, <https://www.ed.gov/media/document/institutional-compliance-section-117-of-higher-education-act-of-1965-october-2020-57158.pdf>

² U.S. Department of Education, Office of the General Counsel, Notice of Investigation to the University of Michigan Pursuant to Section 117 of the Higher Education Act of 1965, July 2025, <https://www.ed.gov/media/document/university-of-michigan-section-117-investigation-letter-july-2025-110399.pdf>

³ U.S. Department of Education, Office of the General Counsel, Notice of Investigation to Harvard University Pursuant to Section 117 of the Higher Education Act of 1965, April 17, 2025, <https://www.ed.gov/media/document/notice-of-investigation-harvard-university-april-17-2025-109861.pdf>

⁴ U.S. Department of Justice, Office of Public Affairs, "Cleveland Clinic to Pay Over \$7 Million to Settle Allegations of Undisclosed Foreign Sources of Funding on NIH Grant Applications and Reports," May 17, 2024, <https://www.justice.gov/usao-ndoh/pr/cleveland-clinic-pay-over-7-million-settle-allegations-undisclosed-foreign-sources>

⁵ U.S. Attorney's Office for the Northern District of New York, "Research Foundation Pays \$313,574 to Resolve Claims That University Research Scientist Failed to Disclose Foreign Support," U.S. Department of Justice, September 12, 2024, <https://www.justice.gov/usao-ndny/pr/research-foundation-pays-313574-resolve-claims-university-research-scientist-failed>

⁶ U.S. Attorney's Office for the District of Maryland, "University of Maryland, College Park Agrees to Pay \$500,000 to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals," U.S. Department of Justice, December 16, 2024, <https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed>

⁷ U.S. Department of Justice, Office of Public Affairs, "Georgia Tech Research Corporation Agrees to Pay \$875,000 to Resolve Civil Cyber-Fraud Litigation," September 30, 2025, <https://www.justice.gov/opa/pr/georgia-tech-research-corporation-agrees-pay-875000-resolve-civil-cyber-fraud-litigation>

⁸ U.S. Attorney's Office for the Northern District of Indiana, "Settlement With Purdue University for False Claims in Research Grant Applications to Federal Agencies," U.S. Department of Justice, November 17, 2023, <https://www.justice.gov/usao-ndin/pr/settlement-purdue-university-false-claims-research-grant-applications-federal-agencies>

⁹ U.S. Attorney's Office for the Northern District of California, "Stanford University Agrees to Pay \$1.9 Million to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals," U.S. Department of Justice, October 2, 2023, <https://www.justice.gov/archives/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign>

¹⁰ U.S. Attorney's Office for the Northern District of Georgia, "Georgia Tech Professor Pleads Guilty to Tax Fraud," U.S. Department of Justice, September 1, 2023, <https://www.justice.gov/usao-ndga/pr/georgia-tech-professor-pleads-guilty-tax-fraud>

¹¹ U.S. Department of Justice, Office of Public Affairs, "Former University of Arkansas Professor Sentenced to a Year and a Day for Lying to Federal Agents About Patents in China," June 16, 2022, <https://www.justice.gov/archives/opa/pr/former-university-arkansas-professor-sentenced-year-and-day-lying-federal-agents-about>

¹² U.S. Department of Justice, Office of Public Affairs, "Jury Convicts Southern Illinois University-Carbondale Professor of Concealing Foreign Bank Account from the Internal Revenue Service," May 6, 2022, <https://www.justice.gov/usao-sdil/pr/jury-convicts-southern-illinois-university-carbondale-professor-concealing-foreign-bank>

¹³ U.S. Department of Justice, Office of Public Affairs, "Jury Convicts University of Kansas Researcher for Hiding Ties to Chinese Government," April 7, 2022, <https://www.justice.gov/archives/opa/pr/jury-convicts-university-kansas-researcher-hiding-ties-chinese-government>

¹⁴ U.S. Department of Justice, Office of Public Affairs, "Harvard University Professor Convicted of Making False Statements and Tax Offenses," December 21, 2021, <https://www.justice.gov/usao-ma/pr/harvard-university-professor-convicted-making-false-statements-and-tax-offenses>

¹⁵ U.S. Department of Justice, Office of Public Affairs, "Georgia Institute of Technology Professor Charged with Visa Fraud and Wire Fraud," March 24, 2021, <https://www.justice.gov/usao-ndga/pr/georgia-institute-technology-professor-charged-visa-and-wire-fraud>

-
- ¹⁶ U.S. Department of Justice, Office of Public Affairs, "MIT Professor Indicted on Charges Relating to Grant Fraud," January 20, 2021, <https://www.justice.gov/usao-ma/pr/mit-professor-indicted-charges-relating-grant-fraud>
- ¹⁷ U.S. Department of Justice, Office of Public Affairs, "Former West Virginia University Professor Pleads Guilty to Fraud That Enabled Him to Participate in the People's Republic of China's 'Thousand Talents Plan,'" March 10, 2020, <https://www.justice.gov/archives/opa/pr/former-west-virginia-university-professor-pleads-guilty-fraud-enabled-him-participate-people>
- ¹⁸ U.S. Department of Justice, Office of Public Affairs, "Former Emory University Professor and Chinese 'Thousand Talents' Participant Convicted and Sentenced for Filing a False Tax Return," <https://www.justice.gov/archives/opa/pr/former-emory-university-professor-and-chinese-thousand-talents-participant-convicted-and>
- ¹⁹ "KU Researcher Concealed Being Recruited for Chinese 'Talent' Program," January 15, 2020, <https://www.justice.gov/usao-ks/pr/new-indictment-ku-researcher-concealed-being-recruited-chinese-talent-program>
- ²⁰ U.S. Department of Justice, Office of Public Affairs, "University Researcher Pleads Guilty to Lying on Grant Applications to Develop Scientific Expertise for China," <https://www.justice.gov/archives/opa/pr/university-researcher-pleads-guilty-lying-grant-applications-develop-scientific-expertise>
- ²¹ U.S. Department of Justice, Office of Public Affairs, "Former Cleveland Clinic Employee and Chinese 'Thousand Talents' Participant Arrested for Wire Fraud," <https://www.justice.gov/archives/opa/pr/former-cleveland-clinic-employee-and-chinese-thousand-talents-participant-arrested-wire-fraud>
- ²² U.S. Department of Justice, Office of Public Affairs, "Researcher at University Arrested for Wire Fraud and Making False Statements About Affiliation with a Chinese University," February 27, 2020, <https://www.justice.gov/archives/opa/pr/researcher-university-arrested-wire-fraud-and-making-false-statements-about-affiliation>
- ²³ U.S. Department of Justice, Office of Public Affairs, "University of Delaware Failed to Disclose Professor's Foreign Government Ties," December 16, 2024, <https://www.justice.gov/opa/pr/university-delaware-failed-disclose-professors-foreign-government-ties>
- ²⁴ Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Research Security," Safeguarding Science, accessed June 10, 2026, <https://www.dni.gov/index.php/safeguarding-science/research-security>
- ²⁵ U.S. Army, "NCSC, ACIC, and Partners Issue New Guidance to Help U.S. Colleges and Universities Mitigate Emerging Foreign Threats to Their Research as School Year Begins," August 2025, https://www.army.mil/article/288081/ncsc_acic_and_partners_issue_new_guidance_to_help_u_s_colleges_and_universities_mitigate_emerging_foreign_threats_to_their_research_as_school_year_begins
- ²⁶ Office of the Director of National Intelligence, National Counterintelligence and Security Center, Safeguarding Academia from the People's Republic of China: A Threat Assessment and Best Practices Guide for Institutions of Higher Education, August 22, 2025, https://www.dni.gov/files/NCSC/documents/products/08222025_Safeguarding-Academia.pdf
- ²⁷ Federal Bureau of Investigation, China: The Risk to Academia (Washington, DC: Federal Bureau of Investigation, 2019), <https://www.fbi.gov/file-repository/counterintelligence/china-risk-to-academia-2019.pdf>
- ²⁸ Christopher G. Pernin, Cortney Weinbaum, Fiona Quimbre, Shanshan Mei, Shay Hershkowitz, Libby Weaver, and Catherine Kish, Research Security in Science and Technology (Santa Monica, CA: RAND Corporation, March 31, 2026)
- ²⁹ Tiffert, G., & Stoff, J. (2021). Eyes wide open: Ethical risks in research collaboration with China. Hoover Institution
- ³⁰ Tiffert, G., Stoff, J., Gamache, K., (2020). Global engagement: Rethinking risk in the research enterprise. Hoover Institution
- ³¹ Jeffrey Stoff, John Sava, and L.J. Eads, Are Research Security Policies in the US Working? A Case Study on Research Collaborations with PRC Defense Laboratories and US Federally Sponsored Research (Council on Research Security and Integrity, February 2026), <https://researchsecurity.org/wp-content/uploads/2026/02/CRSI-IsResSecurityWorking-Final.pdf>
- ³² L.J. Eads and John Sava, Intelligence Compromised: China's Embedded Access to IARPA and U.S. Defense Research (2026), https://static1.squarespace.com/static/6544f8e19664ba2d982d1958/t/699c67dc069cf32d65e21fd0/1771857884536/Intelligence+Compromised_Final.pdf

-
- ³³ Strider Technologies, From Innovation to Weaponisation: How China Exploits the UK Open Scientific System (Strider Technologies, Q4 2025), <https://content.striderintel.com/wp-content/uploads/2025/11/2025-Q4-Innovation-Weaponisation-Report-UK-01-ka.pdf>
- ³⁴ Strider Technologies, Los Alamos Club: How the People's Republic of China Recruited Los Alamos National Laboratory Scientists to Advance Its Military Technologies (Salt Lake City, UT: Strider Technologies, September 2022), <https://content.striderintel.com/wp-content/uploads/2022/09/Strider-Los-Alamos-Report.pdf>
- ³⁵ Institute for Security and Development Policy, "Are Research Security Policies in the U.S. Working? A Case Study on Research Collaborations with PRC Defense Laboratories and U.S. Federally Sponsored Research: An Interview with Jeffrey Stoff, John Sava, and L.J. Eads," April 2026, <https://www.isdp.eu/publication/are-research-security-policies-in-the-u-s-working-a-case-study-on-research-collaborations-with-prc-defense-laboratories-and-u-s-federally-sponsored-research-an-interview-with-jef/>
- ³⁶ Antonia Hmaidi, "Europe's Research Dilemma: Balancing Security and Scientific Cooperation with China," Mercator Institute for China Studies (MERICS), 2026, <https://merics.org/en/comment/europes-research-dilemma-balancing-security-and-scientific-cooperation-china>
- ³⁷ Didi Kirsten Tatlow, Exclusive: U.S. Gave \$30 Million to Top Chinese Scientist Leading China's AI 'Race', Newsweek (Nov. 1, 2023), <https://www.newsweek.com/us-gave-30-million-top-chinese-scientist-leading-chinas-airace-1837772>
- ³⁸ Kate O'Keeffe, "US Funded \$1 Billion in Research with Chinese Labs, Report Says," Bloomberg, February 19, 2026, <https://www.bloomberg.com/news/articles/2026-02-19/us-funded-1-billion-in-research-with-chinese-labs-report-says>
- ³⁹ Garret Molloy and Elsa Johnson, "INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford," Stanford Review, May 7, 2025, <https://stanfordreview.org/>
- ⁴⁰ Stanford Review, "INVESTIGATION: Stanford Receives Chinese State-linked Donations," June 1, 2026, <https://stanfordreview.org/investigation-stanford-receives-chinese-state-linked-donations-2>
- ⁴¹ Neil Ashdown, "The Government Needs to Send a Wake-Up Call on Research Security," December 3, 2025, <https://www.rusi.org/explore-our-research/publications/commentary/government-needs-send-wake-call-research-security>
- ⁴² Government of Canada, "Research Security," Government of Canada, accessed June 10, 2026, <https://www.canada.ca/en/services/defence/researchsecurity.html>
- ⁴³ Masashi Umehara, "Who Pays the Price for Managing China-Related Risks in UK Universities?" March 27, 2026, <https://www.rusi.org/explore-our-research/publications/commentary/who-pays-price-managing-china-related-risks-uk-universities>
- ⁴⁴ UK Research and Innovation, "Trusted Research and Innovation," accessed June 10, 2026, <https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/>
- ⁴⁵ See Appendix for Suspension and Debarment Cases.
- ⁴⁶ James C. Mulvenon and Anna B. Puglisi, eds., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (New York: Routledge, 2013)
- ⁴⁷ William C. Hannas and Didi Kirsten Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (New York: Routledge, 2021)
- ⁴⁸ U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *research Security for America's Future in Space: NASA's Enforcement of the Wolf Amendment*, 2026, <https://files.constantcontact.com/f0eecb46901/01f5f0ea-7b55-42d9-8420-011555a64e9a.pdf>
- ⁴⁹ U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Containment Breach: How the U.S. Department of Energy Failed to Prevent Foreign Adversaries from Accessing Sensitive National Laboratory Research and Infrastructure*, 2025, https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/doe_report_containment_breach_final-v2-compressed.pdf
- ⁵⁰ U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Investigative Report on Joint Institutes: Risks to U.S. Research Security from University Partnerships with China*, 2025, <https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/jointinstitutesreportfinal.pdf>
- ⁵¹ U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *From Ph.D. to PLA: How China's Scholarship Program Helps Build the People's Liberation Army's Military and Technological Capabilities*, 2025,

https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/from-ph.d-to-pla-report_final.pdf

⁵² U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Fox in the Henhouse: How the Department of Defense Has Failed to Prevent Foreign Adversaries from Exploiting U.S. Taxpayer-Funded Research*, September 2025, https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fox-in-the-henhouse-report-compressed_0.pdf

⁵³ U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research*, September 23, 2024, <https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2024-09-23%20Research%20Security%20Report.pdf>

⁵⁴ U.S. Senate, Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans*, Staff Report, November 18, 2019, <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf>

⁵⁵ Select Committee on the CCP Roundtable, *Expert Witnesses: John Sava, Jeff Stoff, Dr. Tim Stearns, Select Committee on the CCP Roundtable on Research Security*, November 2023

⁵⁶ Testimony, Jeff Stoff, RedCliff Enterprises, *Reassessing Threats to US Innovation Posed by China and Implications - Testimony Before the U.S.- China Economic and Security Review Commission for Safeguarding Future Supply Chains - Hearing on "U.S.-China Competition in Global Supply Chains*, June 9, 2022, https://www.uscc.gov/sites/default/files/2022-06/Jeff_Stoff_Testimony.pdf

⁵⁷ Kevin K. Gamache, *Responses to Questions for the Record Submitted by the Senate Select Committee on Intelligence*, September 21, 2022, U.S. Senate Select Committee on Intelligence, <https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-qfr-kgamache-092122.pdf>

⁵⁸ Select Committee meetings with various federal law enforcement entities

⁵⁹ *ibid*

⁶⁰ Select Committee on China, *Law interviews, DOJ civil settlements, and suspension and debarment records*

⁶¹ Congressional Report, Permanent Subcommittee on Investigations-Committee on Homeland Security and Governmental Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (2019), <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf>

⁶² Congressional Report, Permanent Subcommittee on Investigations-Committee on Homeland Security and Governmental Affairs, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (2019), <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf>

⁶³ Internal Select Committee on China Documents, *Production from Letter Sent to NSF on 10-years of China-Related Suspension and Debarments*,

⁶⁴ Congressional Report, The Select Committee on China, *Containment Breach: The U.S. Department of Energy's Failures in Research Security and Protecting Taxpayer-Funded Research from Foreign Exploitation*, December 17, 2025,

<https://chinaselectcommittee.house.gov/media/investigations/containment-breach>

⁶⁵ News Article, Natalie Weger, *The Diamondback*, *UMD pays \$500,000 settlement after allegedly failing to disclose foreign funding*, July 22, 2024, <https://dbknews.com/2024/07/22/umd-pays-500000-settlement-fail-disclose-foreign-funding-research-grant/>

⁶⁶ News Report, Dillon Mullan, *Baltimore Sun*, *University of Maryland pays \$500,000 settlement for allegedly failing to disclose researchers funding from Chinese companies*, July 17, 2024, <https://web.archive.org/web/20240718011836/https://www.baltimoresun.com/2024/07/16/umd-pays-settlement-chinese-companies/>

⁶⁷ DOJ Press Release, United States Attorney's Office-District of Maryland, *University of Maryland, College Park Agrees to Pay \$500,000 to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals*, July 16, 2024, <https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed>

-
- ⁶⁸ Congressional Report, The Select Committee on China and the Committee on Education and Workforce, Compromised Independence: CCP Influence at Harvard University, August 13, 2026, <https://chinaselectcommittee.house.gov/media/press-releases/select-committee-investigation-exposing-ccp-influence-at-harvard-university>
- ⁶⁹ U.S. Dep't of Educ., Notice of 20 U.S.C. § 1011f Investigation to Harvard University (Apr. 17, 2025), <https://fsapartners.ed.gov/sites/default/files/2025-05/NoticeofSec.117InvestigationHarvardApril172025.pdf>
- ⁷⁰ U.S. Dep't of Educ., Notice of 20 U.S.C. § 1011f Investigation and Record Request to Stanford University (Aug. 10, 2020), <https://fsapartners.ed.gov/sites/default/files/2023-04/StanfordUniversityAugust102020.pdf>
- ⁷¹ Association of American Universities, AAU Expresses Concerns on NDAA's SAFE Research Act, October 15, 2025, <https://www.aau.edu/key-issues/aau-expresses-concerns-ndaas-safe-research-act>
- ⁷² Association of American Universities and Association of Public and Land-grant Universities, letter to congressional leadership regarding the SAFE Research Act, October 14, 2025, <https://www.aplu.org/wp-content/uploads/Joint-SAFE-Research-Act-Letter.pdf>
- ⁷³ Website, The Select Committee on China, ICYMI: Moolenaar and Sen. Banks on Countering the CCP's Exploitation of U.S. Academic Research, July 23, 2026, <https://chinaselectcommittee.house.gov/media/press-releases/icymi-moolenaar-and-sen-banks-on-countering-the-ccp-s-exploitation-of-us-academic-research>
- ⁷⁴ Internal Select Committee on China Documents, Production from Letter Sent to NSF on 10-years of China-Related Suspension and Debarments,
- ⁷⁵ Internal Select Committee on China Documents, Production from Letter Sent to NSF on 10-years of China-Related Suspension and Debarments,
- ⁷⁶ Ibid
- ⁷⁷ National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information (Sept. 21, 1985), Ronald Reagan Presidential Library and National Archives, <https://catalog.archives.gov/id/6879779>
- ⁷⁸ Hannas, W. C., & Tatlow, D. K. (2020). China's quest for foreign technology: Beyond espionage. Routledge, pg., 9

