Center for Research Security & Integrity

Written Testimony of Jeffrey Stoff
Founder of the Center for Research Security & Integrity

Before a Hearing of the Senate Foreign Relations Committee
"The Malign Influence of the People's Republic of China at Home and Abroad: Recommendations for Policy Makers"
January 30, 2025

Chairman Risch, Ranking Member Shaheen, and distinguished Members of the Committee:

Thank you for the opportunity to testify today on this critically important topic. Now that I am no longer working in the government, I can speak candidly about the PRC's methods to exploit our research and innovation ecosystem and the failures within both the government and academia to address this problem. The last section of this testimony provides specific recommendations to combat the threats posed by the PRC at home and abroad.

Over the last 15 years, I have focused on China's research and innovation ecosystem and its state-driven knowledge and technology acquisition apparatus. The collection and analysis programs I ran while serving in the government provided insights into China's technology transfer strategies, PRC state-sponsored talent programs, and other methods of PRC influence over research at national laboratories and academic institutions. I worked closely with most federal agencies that fund scientific research - including the National Science Foundation, National Institutes of Health, NASA, the Departments of Defense, Energy, and Commerce - as well as law enforcement and intelligence components. That support has exposed me to a range of deficiencies, vulnerabilities, and failures of the US government and academia, which were a key source of my frustration and the reason I resigned from federal service in 2021 after 18 years.

This testimony catalogs various ways the PRC exploits our R&D ecosystem, acquiring and diverting knowledge for purposes that undermine our national and economic security, and how the PRC violates norms and values of transparency, integrity, and reciprocity regarding scientific research and international research collaborations. I provide specific case examples from my research as well as observations and trends derived from my support to various civil, criminal, and national security investigations when I served in the government; some of this material lacks detail on specific entities as that information is not approved for public release.

Throughout this testimony, I candidly discuss the abject failures of the intelligence and law enforcement communities concerning its ability to protect our innovation ecosystem from China's predations and highlight some structural deficiencies that impede its progress. Equally important, I also highlight US academic institutions' failures to live up to the value system they espouse *and the corrupting and corrosive nature of PRC activities that affect our research enterprise*. Some of this involves raising uncomfortable truths that heretofore have not been discussed in public.

Many of the issues and recommendations discussed in this testimony go beyond the jurisdiction of this committee. One of our impediments is the siloed nature of the Executive Branch, and China's predations transcend the responsibilities or authorities of individual agencies (and legislative oversight committees). We must have the courage to upend the status quo where our collective responsibility has been a collective action problem. The last section of this testimony provides specific recommendations that seek to address some of the problems I highlight. Throughout this testimony, I also pose questions that require further inquiry and policy deliberations before specific actions or recommendations can be made.

Table of Contents

Introduction

Sampling of Challenges and Failures of the US Government

I founded a 501(c)(3) organization, the Center for Research Security & Integrity, in part to address government failures and the structural impediments to knowledge building and threat mitigation. A *non-exhaustive* list of these failures include:

- A focus on pursuing criminal cases to mitigate threats that overlook most of the threats to -- and malign influence over -- our research and innovation ecosystem (especially at earlier research stages) that is subject to minimal regulatory oversight. China's predations often do *not* involve espionage or intellectual property (IP) theft as defined by the US criminal code within fundamental research domains. Messaging by the US government that China is stealing secrets from academia is misleading and misguided.

- A dearth of Chinese language-capable analysts and subject matter experts in the US government has led to a fundamental lack of understanding of the magnitude and complexity of China's state-supported technology acquisition and transfer apparatus.

- Failure of the counterintelligence community to sufficiently adapt to post-Cold War realities. A myopic focus on chasing PRC spies leaves most of our research unprotected as the PRC deploys a range of tactics, infrastructures, and human capital to acquire US technology and knowhow that rarely involve its security services. While I was in the government, my support to counterintelligence elements in the FBI and DoD showed that those offices prioritized criminal investigations over leveraging operational approaches to deny and disrupt PRC state-directed technology transfer activities.

- Failure of the Intelligence Community (IC) to understand, track, analyze, and respond to significant components of PRC's "united front" influence operations that support technology transfer efforts. The US government holds a prevailing view that the Chinese Communist Party's united front is strictly a political influence apparatus.

- A multi-decade descoping and devaluation of open-source intelligence within the IC has led to unaddressed and yawning knowledge gaps, a lack of expertise, and an inability to share information with public and private sectors.

- Similarly, persistent knowledge gaps on PRC academic and commercial entities conducting R&D tied to defense and public security apparatuses limit our ability to identify risks, especially in

critical and emerging technology fields.

- A lack of any significant or material support to US research institutions regarding research security and integrity; the burden of conducting due diligence and risk assessments is placed almost entirely on individual institutions. To date, the US government has been unable to provide a knowledge base, data, or other resources to aid US universities in their risk assessments related to their foreign partners. This situation will hopefully improve with the newly created SECURE Center funded by NSF, but there will be limits to the ways it can support all research institutions.

- Inadequate resources and personnel in Offices of Inspectors General severely constrain their ability to investigate fraud or malign foreign influence or interference in federally sponsored research.

- A lack of understanding of how China has built a massive apparatus to recruit experts globally and exploit US (especially federally funded) research. Experts are primarily targeted by the PRC *after* gaining knowledge and experience overseas. The argument that high percentages of PRC nationals stay in the US after post-graduate education and thus benefit the US is too simplistic; much of China's strategy is to tap into overseas-based experts who "serve in place." Creating incentives to stay with no corresponding protections has allowed the PRC to exploit and influence our research to its benefit with impunity.

Sampling of Methods of PRC Malign Influence and Exploitation of Our Research Ecosystem

The threats and malign influence posed by the PRC on our research and innovation ecosystem and the implications - including the corrupting and corrosive effects - is an under-recognized problem. The scale and scope of PRC influence are largely unknown, but this testimony provides insights into the enormity of the problem. Also note that most advanced nations, particularly our key allies, face many of the same predations from China. Much of the PRC's malign influence activities also undermine the integrity and trust of scientific and engineering research. A *sampling* of some of the threats include:

- Converting or diverting US government-funded research into IP that is commercialized in the PRC that may be in violation of research grants or university terms and conditions or, at minimum, solely benefit the PRC.

- Repurposing US research, including in seemingly innocuous fields like climate change and hearing aid research, to PRC defense programs and weapons system development that can undermine or eliminate US military superiority.

- Directing or redirecting US critical technology research funded by industry and federal and state governments by selectees of PRC talent recruitment programs who are under contract with and tasked by the PRC government.

- Improperly influencing or manipulating federal research grant evaluations and award decisions.

- Applying US research to enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Influencing or co-opting US academics' hiring or sponsoring of PRC national PhD students, postdoctoral fellows, and visiting researchers that circumvent merit-based processes and build talent and training pipelines that overwhelmingly benefit China.
- Establishing or co-opting networks of organizations in the US that enable knowledge transfer, talent recruitment operations, and venture capital investments intended to offshore critical technology to China.
- Influencing or tasking researchers at federal research facilities and laboratories to facilitate formal cooperative agreements with PRC institutions, sometimes violating internal conflicts of interest and ethics policies
- Engaging in behaviors that violate norms of integrity, transparency, reciprocity, and other areas that equate to deception, fraudulent publications, laundering the reputations of foreign research institutions, and numerous other ill effects.

I. US Academia: Vulnerabilities, Misaligned Incentives, Negligence, and Complicity

In some respects, academia has been victimized by China's exploitation and malign influence through vulnerabilities inherent in the open nature of how science is conducted. It is unrealistic to expect individual institutions (and even large technology firms that engage in research) to be able to sufficiently protect themselves against the predations of the PRC party-state and the massive resources and infrastructures it has put in place to target US and allied nations.

Some of China's exploitation comes from a natural evolution of how scientific and engineering research is conducted. Academic institutions have traditionally viewed science as a borderless endeavor; pursuing the frontiers of knowledge and betterment of humanity supersedes transitory geopolitical concerns. Governments in liberal democracies have also shared this view: science and technology diplomacy and academic freedom (and freedom to pursue any partnerships and flows of talent) have greatly benefited technological and economic development and such benefits have in the past outweighed any risks. That principle held true for at least half of a century after the Second World War. But this era of progress was partly due to the fact that allied nations were so much stronger technologically and economically that authoritarian regimes played a very small role -- or even participation in -- the scientific enterprise.

Today, neither academia nor governments of liberal democracies have sufficiently adapted to a contradictory reality: one of the most significant contributors to and participants in the global scientific enterprise is also our greatest adversary and strategic rival: one of the world's largest and most technologically advanced economies is also one of the most oppressive authoritarian regimes in history and has a primary objective of dominating and

displacing the US technologically and militarily to reshape the world order and to preserve Chinese Communist Party (CCP) interests.

But this is not the whole story. An uncomfortable truth is that much of China's efforts to exploit, influence, and corrupt our research ecosystem require at least, in some part, the willing participation by US academia – especially where PRC influence has had the most corrupting and corrosive effects. The reality is US universities are run like businesses: their principal objective and motivation is to generate revenue. Money drives most decisions, not security or integrity. When describing "willing participation," I include in that concept a lack of awareness, negligence in taking responsibility for identifying and mitigating concerns, complicity, willful violations of integrity, and disregard for grant rules and conditions intended to ensure fairness, equity, and responsible allocation of federal resources.

This testimony describes both aspects: the victimization of our research by China through the exploitation of our open system and how US research institutions have enabled (willingly or not) PRC malign influence and exploitation.

Federal funding agencies, law enforcement, and intelligence community (IC) elements have done a good job of raising awareness among universities on national security risks and compliance and integrity concerns. US research institutions understand and recognize that there are real risks and concerns that need to be addressed and mitigated. But this often conflicts with academia's primary goal of attracting sustaining revenue sources (and human capital) from anywhere and anyone. Security and compliance, like the private sector, is a cost burden, not an operational priority. *Consequently, the financial incentives and operations of universities often run counter to US national and economic security interests.*

Many US universities have put research security programs in place, partly due to new requirements stipulated in National Security Presidential Memorandum-33 (NSPM-33). That policy requires research institutions receiving more than $50 million in annual federal funding to certify to funding agencies that the institution has established and operates a research security program, which includes elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training."[1] However, NSPM-33 requirements offer no detail or standards of what a research security program should look like. This can become simply a box-checking exercise for universities to claim they have put in place a program.

National Security Decision Directive 189 (NSDD-189), a policy that has been in place since the 1980s, states that the US government will not restrict sharing or collaboration in fundamental research domains except in rare circumstances where national security concerns require classifying the information. This also means that fundamental research, which is defined as both basic and applied research that is published openly, is not subject to export controls or other regulatory restrictions or oversight. There are currently only two

[1] https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

exceptions where Congress has put in place restrictions concerning fundamental research collaborations with adversarial nations including China.

The first relates to an appropriations law that places "Chinese Funding Restrictions" on NASA (also known as the "Wolf Amendment"), prohibiting recipients of NASA funding from engaging in bilateral participation, collaboration, or coordination with the PRC or Chinese-owned companies, including Chinese universities.[2] Multilateral research exchanges involving China and any additional country are exempt from this restriction. The second is a restriction stipulated in the recently passed FY25 National Defense Authorization Act (NDAA), (Sec. 238) that makes institutions ineligible for Department of Defense funding for fundamental research if the US institution collaborates with a set of PRC entities listed in other provisions of the NDAA (as stipulated in Sec. 1286 of the FY19 NDAA).

All other sources of federal funding currently have no restrictions; researchers and institutions are free to partner, collaborate, establish cooperative programs, etc., with any PRC entity of their choosing. Like other countries except Canada,[3] the government can merely provide guidance on national security risks, but universities can ignore this provided they are compliant with existing federal grant requirements. From a legalistic perspective, there are few incentives for universities to create robust security policies that restrict their fundamental research activities or partnerships.

Research Collaborations of Concern

To be fair, universities rightly point out that most lack the resources, foreign language capabilities, and subject matter expertise on PRC entities and geostrategic concerns to conduct robust due diligence and national/economic security risk assessments; this is a burden placed almost entirely on the research institution. Further complicating this issue are knowledge gaps and the IC's structural impediments (discussed later) that have resulted in insufficient scrutiny of many PRC entities and the level of national security risks they may pose.

What about partnerships and collaborations with PRC entities that are widely known to represent national security risks? The data that follows provides a current snapshot of very high-risk US-China scientific and engineering research collaboration.[4] This data is limited to a *sampling* of military entities, weapons R&D facilities, and select defense-affiliated civilian universities. Such data is not a precise indicator of malign foreign influence; **it is rather intended to demonstrate systemic unwillingness in academia to examine national and economic security risks or ethical concerns regarding their research collaborations with**

---

[2] Pub. L. No. 112-10, § 1340 and Pub. L. No. 112-55, § 539.

[3] The Canadian government issued a policy that will deny federal funding for research grants if that research involves collaborations with specific PRC (and Russian and Iranian) institutions in specified critical technology fields. This policy on "Sensitive Technology Research and Affiliations of Concern" was established in the Fall of 2024. Canadian institutions are still free to collaborate with PRC, Russian, and Iranian entities, but no federal funding would be provided to them.

[4] My testimony focuses on STEM and critical technology areas; I am not addressing PRC research collaboration in most social sciences and humanities disciplines that pose fewer national security risks.

China. Furthermore, the huge scale of these high-risk collaborations suggests dependencies and vulnerabilities that China then exploits.

Tables 1 - 4 break down the number of articles published from 2019 to January 2025, coauthored by researchers from a US-based institution and researchers affiliated with specific PRC entities part of the People's Liberation Army (PLA), subordinate to the Central Military Commission (the CCP organ overseeing the PLA), and select PRC state-owned defense conglomerates. This data reflects collaborations that represent the highest risks to national security. The data was compiled using the *Dimensions* tool by Digital Science that aggregates bibliographic metadata of journal articles, conference proceedings, preprints, patents, and other data related to published research. **Disturbingly, a total of 9,398 unique articles were identified involving coauthors based at US institutions and researchers affiliated with select PRC military institutions in just the past five years. This understates the actual amount of US collaborations with PRC military entities** due to the scoping limitations of this testimony and knowledge gaps discussed later.

Table 1 lists a *sampling* of PRC military medical units that have coauthored the most articles with US partners. This is not an exhaustive list of all US-China collaborations with PRC military medical entities. (Note: totals in these tables may exceed the total number of unique articles as there can be more than one PRC entity listed in the same article)

Table 1: US Institution Collaboration with Select PRC Military Medical Entities

PLA / Central Military Commission Medical Entity	Number of Articles with US-based Coauthors
Chinese PLA General Hospital	1,526
Army Medical University	1,012
Air Force Medical University	888
Academy of Military Medical Sciences	289

Some medical research conducted by these entities may be considered low-risk or beneficial (such as cancer research). However, the PRC party-state does not share the same values and ethical principles as liberal democracies concerning research involving human subjects, and thus even research that is beneficial in nature may be diverted to military or unethical purposes. Examples of where this matters include: China's horrific and well-documented record of human organ harvesting, incarceration of political dissidents in psychiatric hospitals, involuntary collection and use of genetic information for mass surveillance purposes, and medical research with military applications such as fighter pilot and solder performance enhancements and human-computer interfaces for weapons programs, etc.

Consequently, collaborations with PLA medical entities can pose national security, ethical, and reputational risks for US and allied nation collaborators and their funders. It is also worth noting that both the US government and private sector entities are acknowledged as funders of this research (presumably funding the US scientists). Government funders include, but are not limited to: the Agricultural Research Service, Air Force Office of Scientific

Research, Centers for Disease Control and Prevention, Congressionally Directed Medical Research Programs, Defense Threat Reduction Agency, Department of Veterans Affairs, NIH, and NSF. A *sampling* of private companies and foundations credited as funders include Abbott, Amgen, Biogen, Boston Scientific, Bristol-Myers Squibb, Eli Lilly, Intel, Intuitive Surgical, Johnson & Johnson, Medtronic, Pfizer, the American Cancer Society, American Red Cross, Bill & Melinda Gates Foundation, Mayo Clinic, Memorial Sloan Kettering Cancer Center, and the Welch Foundation.

Table 2 lists the number of collaborations with the China Academy of Engineering Physics (CAEP) and a few of its subdivisions that are often named separately in English-language publications, i.e., CAEP is not listed as the parent organization. CAEP is China's nuclear weapons design and production complex, which also includes other advanced weapons, components, and delivery systems.

Table 2: US Institution Collaboration with PRC Nuclear and Advanced Weapons Complex

China Academy of Engineering Physics (CAEP)	Number of Articles with US-based Coauthors
CAEP (including subdivisions naming CAEP as a parent entity)	308
CAEP Subdivisions NOT Stating an Association with CAEP	
Beijing Computational Science Research Center	425
High Pressure Science & Technology Advanced Research	398
Institute of Applied Physics and Computational Mathematics	160
Science and Technology on Surface Physics and Chemistry Laboratory	16

Notes: The Beijing Computational Science Research Center works with (and is possibly subordinate to) the Institute of Applied Physics and Computational Mathematics, also known as CAEP's 9th Institute responsible for numerical / computer simulations for nuclear and other weapons designs. The Science and Technology on Surface Physics and Chemistry Laboratory is subordinate to CAEP's Institute of Nuclear Physics and Chemistry located at CAEP's primary facility in Mianyang.

Table 3 offers a *sampling* (not an exhaustive list) of PLA technical schools whose researchers have collaborated with US entities.

Table 3: US Institution Collaboration with Select PLA Scientific Institutes

PLA / Central Military Commission Entity	Number of Articles with US-based Coauthors
National University of Defense Technology (NUDT)	601
PLA Army Engineering University	69
PLA Information Engineering University	66
PLA Air Force Engineering University	36
PLA Academy of Military Science	32

China Aerodynamics Research and Development Center	29
Naval University of Engineering	19

Notes: The National University of Defense Technology is the PLA's premier scientific and engineering research institution. The China Aerodynamics Research and Development Center is the PLA's premier hypersonics R&D facility, although no English-language source indicates the center is affiliated with the military.

Table 4 offers a *sampling* of US collaboration with some of China's largest state-owned defense conglomerates and a few of their subsidiaries. Subdivisions of these state-owned enterprises have research institutes, some of which house state key laboratories and function like academic institutions. Although some of these firms do engage in civilian research and technology areas, they are run by the PRC central government with a primary mandate to support the PLA through the development of weapons systems and components, including China's missile programs. Even if US researchers can credibly claim that their research is strictly for commercial purposes, collaboration with these PRC defense firms can improve these conglomerates' commercial operations and bolster their financial position. This provides the firms more resources to advance their primary purpose of developing defense or weapons R&D and production programs, strengthening the PLA and emboldening China to become more hostile toward its neighbors, supplying and supporting other autocratic regimes (especially Russia), and challenging US military superiority and deterrence in strategic areas such as the Taiwan Strait and the South China Sea.

Table 4: US Institution Collaboration with Select PRC State-Owned Defense Conglomerates

PRC Defense Enterprise	Number of Articles with US-based Coauthors
China Academy of Space Technology	166
China Electronics Technology Group Corporation	133
China Aerospace Science and Technology Corporation	103
China State Shipbuilding (includes China Shipbuilding Industry Corporation)	77
Aviation Industry Corporation of China	56
China North Industries Group Corporation (NORINCO)	52
China Academy of Launch Vehicle Technology	29
Aero Engine Corporation of China	24
China South Industries Group	21
China Aerospace Science and Industry Corporation	18

Notes: The China Academy of Space Technology and the China Academy of Launch Vehicle Technology are subsidiaries of the China Aerospace Science and Technology Corporation. The China Academy of Launch Vehicle Technology is China's largest R&D and production facility for space launch vehicles, liquid-fueled

surface-to-surface missiles, and solid-fueled surface-to-surface and submarine-launched ballistic missiles.[5] CALT also produces the Dongfeng series of intercontinental ballistic missiles (ICBMs), the latest versions equipped with multiple independent nuclear warheads able to strike Western Europe and the United States.[6]

In addition to PLA institutes and state-owned defense firms, there are groups of civilian universities with a primary mission to support military research and defense industries. These universities are known as the "Seven Sons of National Defense" and the "Seven Sons of Ordnance Industry" (two of these schools belong to both groups). The former group of entities originated as military academies but are now directly overseen by the State Administration for Science & Technology Industry for National Defense, the PRC government organ responsible for implementing military-civil fusion policies. These universities work on classified defense programs, house departments and laboratories that work closely with PLA organs, and partner with state-owned defense conglomerates. The universities in the latter group were previously under the supervision of the then Ministry of Ordnance Industry and continue to conduct weapons R&D as part of their core mission.

Some STEM research conducted at these universities are in civilian sectors or may lack obvious defense applications; however, it is prudent to assume that these schools will pursue potential military applications as a matter of policy and thus represent high national security risks. There were 17,630 unique articles published between 2019 and January 2025 involving a coauthor from one of these 'seven sons' defense universities and a coauthor affiliated with a US institution.[7] Table 5 lists the number of articles involving coauthors from these schools and US institutions.

Table 5: US Institution Collaboration with PRC 'Seven Sons' Universities

Seven Sons of National Defense, Seven Sons of Ordnance Industry Universities	Number of Articles with US-based Coauthors
Beihang University	4,909
Harbin Institute of Technology	3,836
Beijing Institute of Technology	3,335
Northwestern Polytechnical University	2,396
Nanjing University of Science and Technology	1,770
Nanjing University of Aeronautics and Astronautics	1,507
Harbin Engineering University	723
North University of China	356
Chongqing University of Technology	208

[5] "China Academy of Launch Vehicle Technology (CALT)," Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59/.
[6] "China Academy of Launch Vehicle Technology – CALT 1st Academy," https://www.globalsecurity.org/wmd/world/china/calt.htm.
[7] Articles involving hyper-coauthorship (that list 100 or more coauthors) were excluded. Many articles also list more than one 'seven sons' schools, so the totals in this table exceed the total of unique articles.

Changchun University of Science and Technology	127
Shenyang Ligong University	53

The data in the above tables are admittedly a crude measure.[8] The statistics provide no indication of the nature or frequency of the US collaborations, which are often informal and sometimes unbeknownst to their federal sponsors or even the US employers. Investigating these collaborations for approximately 27,000 articles is a daunting task. Additionally, as discussed in the knowledge gaps section of this testimony, this data significantly under-represents the number of collaborations posing national security risks: there are many defense and state key laboratories, Chinese Academy of Sciences institutes, subdivisions of civilian universities, and research institutes subordinate to state-owned enterprises that also conduct defense research but have not been compiled in this dataset.

Nevertheless, this cursory survey of US research collaboration with high-risk entities demonstrates academia's widespread disregard for national security concerns, despite the increased scrutiny the US government has placed on these PRC institutions and its outreach efforts to academia. Also note that many of the publications in this data involve other country participation - especially NATO and Five Eyes allies. In 2023, I published a large study that cataloged and assessed German research collaboration with China that also illustrated extensive partnerships with these same PRC entities listed in Tables 1 through 5.

Academia has argued that per NSDD-189, most "fundamental research" should remain unrestricted and any additional rules federal agencies place on international collaborations in fundamental research domains would stifle innovation and cause more harm than it seeks to address. Fundamental research includes both basic and applied research that is published. *But who decides if/when research that is more applied in nature crosses into areas that pose sufficient risk to warrant some form of restriction?* This appears to be arbitrary and largely at the discretion of the individual researcher. Some applied research, especially Department of Defense (DoD)-funded projects that can be sensitive, require significantly more administrative oversight (and restrictions) on who is authorized to conduct the research, who has access to the data and research, dissemination rules on publications (e.g., controlled unclassified information designations), etc.

The incentive is to avoid these issues by publishing openly and, thus, by default, designating the research as fundamental. I lack the technical expertise to make such determinations, but some published research funded by DoD involves very specific applications and raises questions on whether it makes sense to publish that research openly. A recent report by the House Select Committee on China provided examples of research disciplines involving US collaborations with China that appear highly applied and intended for the US military. After all, DoD-funded research is intended to produce breakthroughs for war-fighting capabilities. The report noted:

[8] This data excludes Chinese-language publications appearing in domestic PRC sources and probably understate the actual number of coauthored publications.

"These studies found that the relevant collaborations covered a wide range of sensitive technologies crucial to national security, including cryptography, eavesdropping, hyperspectral imaging, lithium-ion batteries, aerodynamic angles of attack, electronic warfare, cyber-attack detection, high-density explosives, high entropy alloys, radar target detection, quadcopters, artificial intelligence, quantum technology, multi-target tracking, missile impact penetration, and surveillance technologies."[9]

Should all of those articles have been published openly? Should any PRC institution be allowed to materially support or partner with the US in these research areas?

PRC's exploitation of US federally funded research also goes far beyond just DoD-funded research projects. Entities such as the Department of Energy also fund research in nuclear, weapons and energy development that are dual-use technologies. The same is true for NSF, which funds research on radar, underwater acoustics, artificial intelligence, and many other areas with obvious dual-use applications. Even NIH funding is at risk. My research on US and German collaborations with China revealed multiple instances where scientists developing advanced hearing aids using signal and speech processing techniques funded by NIH had dual appointments and/or work with a PLA Navy underwater warfare research division of Northwestern Polytechnical University and a defense laboratory on radar signal processing at Xidian University (which is co-supervised by China's largest defense electronics and radar systems developer).

Does NIH have the ability or mandate to evaluate potential national security risks associated with every grant it awards involving health or medical research? Should they? Does the DoD have jurisdiction over NIH grant award decisions or monitor this type of activity? Should they?

Patents: Directing or Diverting US Innovation for China's Benefit

Another way to observe how China exploits our research ecosystem to gain knowledge, experience, and technology that can be commercialized and weaponized in China is by surveying patent filings, specifically patents filed in China and/or that have PRC organizations as the patent assignee or co-assignee. **The apparent blind spots on the scale and scope of this phenomenon also mean we have little insight into how and why some of the patents are filed in China by US academics.** One US university compliance official told me that he knows of some faculty members who have only filed patents in China their entire academic careers at that US university - they have never filed patents in the US. Additionally, government investigations of PRC talent programs (discussed in a later section) have uncovered contracts mandating that all intellectual property generated from research by program selectees will be exclusively owned by China. Filing patents with PRC assignees may meet this requirement.

Comprehensive analyses and assessments of patents exceed the scope of this testimony and my area of expertise. I merely provide a sampling of patent records that sufficiently

[9] "CCP on the Quad: How American Taxpayers and Universities Fund the CCP's Advanced Military and Technological Research," House Select Committee on the CCP, Sep. 2024.

raise serious concerns and policy questions and, once again, suggest negligence or indifference by US universities.

To survey a sampling of data, I compiled patent filing metadata records using the *Dimensions* tool courtesy of Digital Science, where a listed co-inventor has/had an association with select US universities. I chose some of the most research-intensive universities based on the assumption that there would be more patent data available and that some of the patents could have resulted from federally funded research. Using usaspending.gov, I compiled the top 10 recipients of federal grants (excluding contracts) reported for Fiscal Year 2024. The universities and the total amounts of grants received are:

1. University of California, San Francisco ($964.8M)
2. University of Washington ($929.2M)
3. Johns Hopkins University ($893.9M)
4. Columbia University ($839.1M)
5. University of Wisconsin ($810.4M)
6. University of Pennsylvania ($803.4M)
7. Stanford University ($771.5M)
8. Washington University in St. Louis ($766.3M)
9. University of Pittsburgh ($744.2M)
10. Yale University ($731.4M)

I limited patent records to those filed within the past 5 years (2019-present) that have the following criteria:

- List a co-inventor who had a recent affiliation with one of the 10 US universities listed above.[10]
- Name at least one China-based organization assigned to the patent (assignee) **that the US government has determined poses a national security risk.** These include entities on the BIS Entity List, DoD-designated military-affiliated organizations (as stipulated in Sections 1286 and 1260H of the NDAA), or entities sanctioned by the Treasury Department's Office of Foreign Assets Control (OFAC).
- Patents records that appear current and valid (based on the *Dimensions* data); i.e., patents that have a legal status of being pending, granted, or active. Patents marked as abandoned, ceased, expired, or withdrawn were removed.[11]
- The number of co-inventors in these tables is broken down by researchers who appear to maintain a current affiliation with the US university and those who had some affiliation with the US university in the past five years.

This data is a cursory survey, and there are limitations that almost certainly result in an underrepresentation of the actual number of patents filed. For instance, only PRC entities on *current* US government entity lists were used; there are other PRC research-performing organizations that support defense research that warrant inclusion on US government lists.

[10] Dimensions relies on publication, grant, and clinical trial information to assign a co-inventor's affiliation. A lack of records and publishing timelines (delays) may not accurately reflect an individual's most current affiliation.
[11] A small percentage of the patent records lack information on legal status (marked N/A); I chose to include those records.

Additionally, I cannot characterize the nature of each of the co-inventors' previous and current affiliations/employment due to scoping limitations. There are many co-inventors in this data that no longer have an affiliation with the US university in question; some of these individuals were probably visiting scholars and postdoctoral researchers who did not have full-time or permanent employment status with the US institution. More in-depth research is needed to determine the nature of the US affiliations or whether any of the co-inventors were recipients of federal research grants.[12]

Table 6: Patents Dated 2019-2025 Listing PRC Assignee on US Restricted Lists

US University	Number of (co-)Inventors Recently Associated with US University	Number of (co-)Inventors Currently Affiliated with US University	Number of Patents with (co-)Inventor Currently Affiliated with US University	Total Patents with PRC Assignees on Restricted Lists
University of California, San Francisco	41	5	13	199
University of Washington (includes Applied Physics Laboratory)	66	3	4	338
Johns Hopkins University (includes Applied Physics Laboratory)	110	9	26	350
Columbia University	63	14	92	441
University of Wisconsin - Madison	66	4	23	395
University of Pennsylvania	65	10	21	273
Stanford University	113	17	31	388
Washington University in St. Louis	38	14	34	307
University of Pittsburgh	63	7	18	271
Yale University	82	6	31	383
Totals	**707**	**89**	**293**	**3,345**

[12] In a few observed cases, the patent filing actually credits US federal funding support, but that is rare.

Despite these scoping limitations, this data covering the past 5 years is alarming: **it shows that 89 researchers who appear to be currently affiliated with these 10 universities have filed 293 patents with a PRC assignee organization the US government has placed sanctioned or restrictions on**; a **total of 3,345 patents filed with high-risk PRC assignees list a co-inventor who had a recent affiliation with these US universities.** We do not know how pervasive this is across the research community. Technical analyses of these patent records would help determine the nature of the proposed technology and provide insights into specific research areas China seeks to turn into practical applications.

A simple scan of patent records can sometimes be revealing without relying on technical analysis. Patents listing two co-inventors associated with Johns Hopkins University (one of whom claimed an affiliation with the university as recently as June 2024; the other appears to have held a visiting scholar position and left in 2023), are quite concerning: the filing dates appear to overlap with the co-inventors' association with Johns Hopkins and the titles suggest military applications. The assignee of the first patent listed below is a university extensively involved in PLA Navy and Air Force research; the second university is principally engaged in microelectronics, radar systems, and other technical infrastructure for the PLA and China's largest defense electronics firm.

Patent CN-111190430-B: "Unmanned aerial vehicle suspension load control method using tether rotor coordination," assignee: Northwestern Polytechnical University

Patent CN-113111786-B: "Underwater target identification method based on small sample training diagram convolutional network," assignee: Xidian University

For individuals who lack policy expertise on patents (including me), this data and its implications raise numerous questions, such as:

- How and why did a US researcher file a Chinese patent, i.e., what motivations, incentives, or taskings by PRC entities were involved that may indicate malign PRC influence?
- What are appropriate policy measures individual research institutions, federal funding agencies, and foreign policy elements of the government should take when US academics file a patent where the only assignee is a PRC institution? Would policies differ depending on the PRC entity involved, e.g., if the patent assignees are on US restricted lists?
- To what extent are university administrators and government agencies aware of this activity taking place? If the universities are aware, are there formal licensing or revenue sharing agreements or contracts in place, especially if a patent has both a US and PRC co-assignee? If so, would such arrangements create compliance issues with federal funding agencies or export controls (when the patent assignee is on the BIS Entity List)?
- What monitoring and oversight mechanisms are in place, if any, to identify, assess, and mitigate national **and** economic security when patents are filed in China and/or with China-based (co-)assignees?

Ethical Risks in PRC Research Collaborations

The previous section sampled *some* US-China research collaborations that pose very high national security risks yet receive little regulatory oversight. Academia's indifference to such

concerns is not limited to national (and economic) security concerns that run counter to the national interests of the US. This section demonstrates the *ongoing indifference or lack of awareness by academia of the ethical risks of research collaborations with China.* I am referring to collaborations that involve research disciplines that are intended for or can be diverted to mass surveillance technologies or involve partnerships with PRC research institutions that support the CCP's public security apparatus that engages in human rights abuses. I exclude from this discussion ethical concerns regarding how the research is conducted, particularly as it relates to human subjects due to my lack of knowledge in that area.

A study I published with the Hoover Institution examined the Chinese Academy of Sciences Institute of Automation (CASIA), one of China's premier AI, computer vision, and neuroscience research institutes. CASIA enjoys global collaboration with academia and industry, including major technology firms like Google, Dell, and Intel. Yet CASIA is extensively involved in developing and commercializing mass surveillance technologies, including facial, iris, and gait recognition, and video surveillance. CASIA owns commercial spinoffs that have developed these surveillance technologies for PRC public security organs, including for use in the Xinjiang region used to oppress and detain Muslim minority populations.[13]

I compiled data on US collaborations involving US-based coauthors alongside CASIA researchers published from 2019 to January 2025 and found 676 unique articles. US collaborations with CASIA appear to continue unabated, suggesting academia is not concerned with the ethical or reputational risks of working with CASIA.

CASIA is just one organization in China that extensively supports the party-state's surveillance apparatus and corresponding human rights abuses. To survey a larger set of ethically troubling research collaborations, I compiled bibliographic metadata on scientific publications whose abstracts contained one or more of the following keywords that have obvious surveillance applications:

- biometrics
- facial identification
- facial recognition
- iris recognition
- gait recognition
- pose estimation
- person tracking
- person re-identification
- video surveillance
- scene understanding

[13] See Stoff, Tiffert, "Eyes Wide Open: Ethical Risks to Research Collaboration with China," *Hoover Institution*, December 2021, https://www.hoover.org/sites/default/files/research/docs/stoff-tiffert_eyeswideopen_web_revised.pdf.

- emotion recognition
- expression recognition

Researchers from the US and other nations that collaborate with China on topics related to these areas may be focused on innocuous, commercial applications. However, when PRC institutions partner in these research disciplines, we must assume they may be seeking mass surveillance applications that can benefit the PRC's public security apparatus or, in some cases, may be subordinate to or a supplier of PRC public security organs. Table 7 shows the results of collected publication metadata that have abstracts involving one of the keywords listed above. The table shows the number of articles naming a coauthor from China and a coauthor from another nation ranked by the total number of articles.

US-based coauthors are the largest collaborators with China in these surveillance-related disciplines, but US dominance may also be a function of its size as the world's largest or 2nd largest producer of scientific publications annually. Regardless, *the data here is a small sampling* of articles that are easy to recognize as raising ethical concerns. More scholarship is needed that builds comprehensive keyword ontologies associated with research disciplines with potential surveillance use, the PRC research institutions involved, and the foreign collaborators.

Table 7: Top 10 Countries Coauthoring Articles on Surveillance Research with PRC Institutions (articles published 2020- Jan. 2025)

Country	Number of Articles
USA	1,472
Australia	633
Singapore	539
Japan	438
Canada	419
Germany	317
India	220
UK	219
Italy	161
France	157

Collaborations in these ethically troubling areas that can enable or enhance China's surveillance and oppression of its citizens *and* the export of related technologies to authoritarian regimes around the world raise important questions for governments and policymakers:

- Given a lack of regulatory oversight regarding fundamental research, what policy changes (if any) should be made to disincentivize universities and firms from engaging in ethically troubling collaborations with China? For instance, is it OK for researchers at IBM to collaborate with researchers from the *People's Daily* - China's official newspaper of the CCP that is a propaganda tool for both domestic and foreign messaging purposes?[14]

- What if the US-based researchers who work with the PRC on surveillance disciplines are recipients of federal funding, such as NSF, DoD, NIH, and the Office of the Director of National Intelligence? **All of these agencies were** acknowledged as funders in some of the publications that formed the basis of Table 7.

- Do program managers at federal agencies have a set of ethical guidelines when awarding grants on this type of research separate from ethical review boards, which only address

[14] See https://dl.acm.org/doi/10.1145/3474085.3478574.

research that directly involves human subjects?

- Who is monitoring formal and informal research partnerships and exchanges between US institutions and PRC entities in areas that have clear surveillance applications and that can enable human rights abuses?[15] Do universities have a set of ethical guidelines or values that discourage or prohibit collaborations with authoritarian nations in these research areas?

Malign Influence from PRC Funding and Resources

Up to this point, I have focused on problematic research collaborations that can lead to exploitation by China, including diverting or applying such research for military or surveillance use. The massive amount of concerning collaborations, as reflected in publications and patent records should be framed within the context of malign PRC influence because China's partnerships with the US often serve a much different and dangerous purpose than the intentions, norms, and values of the US partners. That also holds true with China's collaborations with allied nations. *This section describes a more explicitly malign influence activity that has profound corrupting and corrosive effects, some of which have not been discussed in public given the associated compliance and reputational risks: PRC funding and resources provided to US research institutions.*

In oversimplified terms, US universities run like businesses in that their primary objective is to bring in revenue. This is partly due to the fact the federal and state governments do not provide enough funding to universities for them to operate; academia must rely on a diverse set of revenue sources. This creates inherent vulnerabilities that foreign entities - especially the PRC - can exploit for their benefit and create incentives that are often not aligned with US national interests. An uncomfortable truth is that US universities have a history of accepting gifts, contracts, and grants from nearly any entity in the world without discrimination (or due diligence) on those funders.

Section 117 of the Higher Education Act requires institutions that receive any form of federal funding to disclose foreign sources of funding to the US Department of Education on a biannual basis.[16] However, both Congressional and Department of Education investigations found widespread non-compliance with this law. An early 2019 report by the US Senate Permanent Subcommittee on Investigations found that foreign funding in America's higher education system is "effectively a black hole," with up to 70% of colleges and universities failing to disclose mandatory foreign funding.[17] A report issued in late 2020 by the Department of Education revealed more than $6.5 billion in previously undisclosed foreign

---

[15] PRC institutions extensively involved in surveillance research and support or are part of public security organs is a knowledge gap – arguably another failure by the IC to systematically identify such entities and share that information with the public. BIS does add companies to the Entity List that demonstrate they contract with or supply PRC public security organs, but few, if any, efforts have been made that look at PRC academic institutions.

[16] See 20 U.S. Code § 1011f.

[17] "China's Impact on the U.S. Education System," U.S. Senate Permanent Subcommittee on Investigations (Feb. 2019), www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20Report%20China's%20Impact%20on%20the%20US%20Education%20System.pdf.

funding (from China, Russia, Iran, and Qatar) and found that "historically, fewer than 300 of the approximately 6,000 U.S. institutions self-report foreign money each year."[18]

What follows is a discussion of specific cases and observations from my experience supporting PRC influence investigations when I was in the government. **What is usually missing from public discourse related to these issues are the secondary effects and implications that undermine integrity, trust, fairness, and equity in our institutions of higher education.** US academic institutions are naturally not monolithic, and I do not suggest every institution operates in the same unscrupulous ways described here. There are some universities, for example, with robust research security and compliance programs that seek to serve as responsible stewards of taxpayer money.

Case Examples

The first set of cases relates to PRC firms sponsoring research in non-transparent ways that undermine research security and integrity and have led to non-compliance on federal research grants. Like other threats and challenges, this phenomenon is not unique to the US. Canadian media revealed multiple agreements between Canadian universities and PRC technology giant Huawei that totaled more than $50 million, and those agreements required that all intellectual property rights born out of the collaboration belong solely to Huawei.[19] Huawei has built R&D centers around the world and sponsors research in academia. However, the conglomerate has come under scrutiny from Five Eyes nations and key EU allies due to its reported ties to PRC military, intelligence, and public security organs. Additionally, the US government placed Huawei on the BIS Entity List that restricts exports, and the company has been accused by the Department of Justice of committing intellectual property theft, obstruction of justice, and fraud related to the evasion of US sanctions against Iran.

In essence, the Canadian universities performed contracted research for China. Besides having no real benefit to the universities or Canada other than a temporary source of revenue, it is even more problematic when some of that research and facilities are supported by federal funding. What about in the US? What do Huawei and other PRC sponsorship agreements with US research institutions look like? Given the widespread disclosure failures of foreign funding by US institutions, this is largely unknown. Some US media sources have exposed a few examples where PRC surveillance technology firms like SenseTime and Megvii have partnered with US universities. There are two recent cases that also shed some light on this.

US Research Institutions and Huawei

In a case uncovered by *Bloomberg*, Huawei provided funding to Optica Foundation, a US-based non-profit organization. Optica then awarded research grants to academics while not

---

[18] "Institutional Compliance with Section 117 of the Higher Education Act of 1965," U.S. Department of Education, Office of the General Counsel (Oct. 2020), www.ed.gov/sites/ed/files/policy/highered/leg/institutional-compliance-section-117.pdf.
[19] Robert Fife and Steven Chase, "Huawei Still Filing Patents Tied to Work with Canadian Universities after Ottawa's Restrictions," *Globe and Mail,* November 9, 2023, www.theglobeandmail.com/politics/article-huawei-canadian-universities-patents/#:~:text=In%20the%20past%20two%20years,University%20of%20British%20Columbia%20and.

disclosing that Huawei was the source of funding. Optica Foundation sponsored a research competition that awards a total of $1 million per year to winners to conduct research on a specific area. According to the *Bloomberg* report, universities, applicants, and even one of the competition's judges were unaware that Huawei was the source of funding. *Bloomberg* reviewed a "non-public document" that appears to be the contract between Huawei and Optica Foundation. The document included a provision stating that the existence of the agreement and all details contained therein shall be considered confidential information.[20] Thus, Huawei used a third-party professional society (Optica Foundation) as its proxy to hold multi-year contests to grant researchers funding on specific projects in a secretive way. This was almost certainly intended to avoid scrutiny by not having to provide funding to universities directly.

In July of 2024, the University of Maryland (UMD) entered into a settlement agreement with the Department of Justice that also involved funding from Huawei. The United States alleged that UMD "knowingly failed to disclose current and pending foreign funding that three UMD researchers had sought and received, in five research grant proposals submitted to the NSF and the Army. Specifically, the United States alleged that UMD failed to disclose to NSF gift funding from Huawei Technologies Co., Ltd. to a PI[21] for research in 'high energy density FeF3 conversion cathode materials and Li metal anodes.'" The government also alleged that UMD failed to disclose to the NSF and Army funding provided to two other PIs from Taobao (China) Software Co, a subsidiary of Alibaba titled, "Large-Scale Behavior Learning for Dense Crowds" and "Cyber-Manufacturing of Customized Apparel."[22] Note that the first project clearly has mass surveillance applications.

This UMD case appears to be consistent with other investigations I supported when I was in the government, where PRC entities basically contract with US academia to conduct research on specific projects led by specific PIs. Yet the recipient US institutions claim those sources of funding are unrestricted gifts, meaning that they are donations to US institutions that are free to use the funds in any way they see fit. Academia has argued that it does not have to report that as current or pending support on federal grant applications because those "gifts" do not relate specifically to the research grants.

In at least some observed cases, these gifts are really contracts or grants in disguise; they "recommend" specific US faculty work on specific research projects at the PRC's behest. PRC institutions are directing US institutions to perform research by specific personnel. Naturally, US universities will abide by the wishes of the PRC "donors" to avoid jeopardizing those revenue streams.

A secondary compliance concern may also be taking place. Unrestricted gifts may not have to be counted when universities calculate the administrative/overhead costs associated with the federal grants they receive. Universities charge a portion of each federal grant to

---

[20] Kate O'Keeffe, "Huawei Secretly Backs US Research, Awarding Millions in Prizes," *Bloomberg,* May 2, 2024, https://www.bloomberg.com/news/articles/2024-05-02/huawei-secretly-backs-us-based-research-with-millions-in-prizes-through-dc-group?srnd=undefined.

[21] PI refers to principal investigator, the researcher(s) that leads a project funded by federal research grants.

[22] https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed

cover the administrative costs of executing the research. The implication is that if a university receives a federal grant to perform research that is materially similar to the research sponsored by a "gift," then in essence, the university may be overcharging the US government on its administrative costs. That may be considered fraud - a violation of the False Claims Act.

One observed way PRC entities funnel money into US academic institutions is through US academics that hold concurrent positions at PRC universities (such as visiting professors), often recruited through one of the hundreds of PRC state-sponsored talent programs described in the next section of this testimony. The US academics holding these PRC positions then serve as a proxy for PRC institutions, brokering gifts, contracts, grants, and cooperative agreements with the US institutions where they are employed.

Stanford's Settlement of False Claims

In another settlement, the United States alleged that on 16 grant proposals submitted to the Army, Navy, NASA, and NSF, Stanford University "knowingly failed to disclose current and pending foreign funding that 11 Stanford PIs and co-PIs had received or expected to receive in direct support of their research." The United States further alleged that Stanford "knowingly failed to disclose to the Army, Air Force, and NSF that a Stanford professor received research funding in connection with his employment at China's Fudan University and from a foreign government's national science foundation" (refers to the PRC).[23] The US alleges that these disclosure failures violate the False Claims Act.

Federal agencies require grant applicants to disclose all current and pending support received by the institution and the PIs and co-PIs on the grant proposals. Current and pending support is defined as all resources from any source - including foreign governments- that are made available to researchers in support of their research endeavors.

Interagency efforts to pursue civil remedies should be lauded as they are a more effective and fairer approach to mitigating these concerns compared to pursuing criminal prosecutions. In the Stanford case, the settlement agreement required Stanford to pay $1.9 million to resolve allegations of False Claims Act violations. However, a cursory survey of the grants listed in the settlement agreement that were (allegedly) fraudulent totaled over $14 million. The False Claims Act allows for damages of *up to triple* the amount of the federal grants, plus a flat penalty per occurrence of each false claim submission. Consequently, these small settlement agreements are unlikely to create any real deterrent for universities to change their behavior. The penalties have been a modest cost of doing business, and universities can maintain the status quo of receiving an unknown amount of funding and support from PRC entities and, in essence, "double-dip" by taking federal grant dollars to do the same research.

There are secondary and corrosive effects that are not being discussed. When universities or their faculty fail to disclose these outside sources of funding (regardless of whether they are

[23] https://www.justice.gov/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign

characterized as gifts, grants, or contracts), that affects federal grant award decisions. This violates the principles of integrity and transparency that universities espouse as core values. Federal research grants are highly competitive as only a fraction of the total submissions are usually awarded. There are finite taxpayer dollars; if universities are, in essence, double-dipping by taking both PRC and US government funding, this means that other universities – especially those with fewer resources like smaller institutions and Historically Black Colleges and Universities -- are denied those federal research dollars that could have otherwise been awarded.

This creates a vicious cycle of inequity in the system: schools that are being honest but denied federal funding means they have smaller budgets and fewer resources to hire PhD students, attract top talent, etc., which then makes them less competitive on future grant proposals. This also translates to fewer opportunities domestically.

How pervasive is this problem, and how much PRC funding and resources are being funneled to (and hidden by) US universities? *In addition to the corrosive effects described above, a lack of awareness of this problem means it is impossible to determine the level of influence the PRC is exerting over the conduct of US research that may be overwhelmingly (or unilaterally) benefitting China to our detriment.*

II. Understanding PRC Talent Programs Beyond Research Security: Integrity and Malign Influence Matters

PRC state-sponsored talent recruitment programs number in the hundreds and play an instrumental role in China's economic development and military modernization efforts. They

> "Overseas returnee scientists are the talent power behind knowledge and technology transfers and have gradually become China's new force in academic development and S&T innovation, promoters of high and new technology applications, and frontrunners in promoting China's innovative development." (A "responsible person" who is a member of the CCP Central Committee Talent Work Coordination Small Group, the key policy body on talent recruitment programs in a Xinhua article - 海归梦, 中国梦," November 7, 2017, www.xinhuanet.com//mrdx/2017-11/07/c_136733044.htm)

are statutorily designed to transfer technology and knowhow from overseas through any and all means at the PRC party-state's disposal. There has been considerable US government scrutiny on these programs - often described in various policies as "malign foreign talent recruitment programs" to differentiate them from scholarships and talent programs of other nations. Federal agencies have exerted considerable efforts to explain to academia and the private sector the national and economic security risks these programs pose. Primers on the PRC's talent programs have been published elsewhere and thus are not included in this testimony. The focus of this testimony is the features and activities of these programs that intersect with malign influence and research integrity concerns.

Some institutions in the US and EU have downplayed the risks and threats posed by China's state-sponsored talent programs and view the US government's concerns as overblown. Some arguments center around the mirror imaging of our systems with the PRC - that most countries have talent promotion programs of various kinds, such as government-sponsored fellowships and scholarships that send citizens abroad to gain knowledge and experience and attract talent from the international community to further domestic endeavors. At a basic level, the goals of many government-led human capital investments are indeed similar to those of the PRC: to help advance science and technology to bolster a country's economic development.

However, this argument overlooks key differences between programs in allied democracies and those in the PRC concerning the methods, requirements, supporting infrastructures, and how PRC talent programs integrate into and support a state-directed strategy to acquire technology and knowhow from around the world. The arguments downplaying the risks also overlook China's system of governance and *rule-by-law* approaches. This is particularly relevant as PRC talent program selectees, regardless of nationality, are under contract with the PRC government: they are tasked and funded by party-state organs and subject to PRC law.

Another structural difference between China's talent programs and other nations relates to scale and scope. PRC programs, in addition to their sheer size and number, have supporting infrastructures and ecosystems, such as:

- Dedicated research funding lines
- Venture capital investment structures
- Global recruitment and candidate evaluation networks
- Government-run databases of overseas experts used for targeting
- Co-opted domestic and overseas support organizations, many of which are part of China's United Front influence apparatus

There are other elements of PRC talent programs that encourage insidious behaviors, many of which should be viewed as malign foreign influence. Selectees of these programs can have corrupting effects on our academic institutions, exploit individual and institutional vulnerabilities through money and resources; undermine values of academic research, such as integrity and transparency; create conflicts of interests or conflicts of commitment; and incentivize intellectual dishonesty and academic fraud. Depending on the academic institution, administrators have been unaware, turn a blind eye to (or admit they do not want to know), or are complicit; all of which demonstrate the corrosive nature of China's influence.

Talent program selectees have requirements that undermine our values system beyond national security threats, including:

- Attribute awards, patents, and projects to PRC entities, even if the research used US funding
- Recruit and train specific individuals: coordinate with the PRC government to hire/sponsor PRC nationals to come to the US and circumvent merit-based hiring processes; recruit others

into talent plans

- Fail to inform US employers of their commitments in the PRC; redact information on faculty pages and CVs related to talent program appointments or use innocuous or alternative titles such as “honorary” or “visiting professor,” “advisor,” or “academic committee member” when actually serving in a talent program-sponsored position

- Replicate or transfer US-funded research to the PRC or request duplicative grant funding from PRC and US sources on the same research

- Retain positions in the US and concurrently advise or lead research efforts in the PRC; direct, divert, or influence R&D for China’s benefit, such as running parallel labs in the PRC

- Facilitate the brokering of gifts, grants, cooperative agreements, joint PhD training programs, or other contracts between US and PRC institutions

Case Example 1: Corrupting NOAA Research and Operations

An investigation I supported when I was in the government illustrates the various ways talent programs can involve malign influence and create corrosive effects on our research. This case is also important because it shows federal research facilities are also affected, not just universities. The US government pursued a criminal investigation in part because the subject was a federal employee - a climate scientist at the National Oceanic & Atmospheric Administration (NOAA). The scientist was recruited through two nationally run PRC talent programs to take a part-time position at a PRC university while retaining his full-time employment with NOAA. The criminal elements of the case centered around prohibitions against government employees taking outside, concurrent employment (especially with a foreign government).

However, the requirements of the PRC talent program appointments were the most concerning with respect to malign influence, some of which are not illicit. For instance, the NOAA researcher’s contracts with the PRC government obligated him to:

- Sponsor specific PRC national researchers to work in his NOAA lab *as directed by the PRC*. The subject failed to evaluate multiple candidates for these positions as required; he bypassed merit-based hiring processes and systematically denied US applicants.

- Work on research projects at NOAA as determined by his PRC sponsors; collaborate on PRC government-funded research projects with specific scientists using NOAA facilities.

- Travel to and work in China for two full months per year, which exceeded federal annual leave accruals. This meant the researcher was certifying time and attendance reports that he was working at NOAA and lying to his supervisors about his China-based commitments.

- Publish research that credited the PRC institution as the primary affiliation, even if the research was principally (or entirely) conducted at NOAA facilities. A literature review showed that the scientist published some papers listing his NOAA affiliation and other papers listing him as exclusively affiliated with a PRC institution during his tenure at NOAA.

- "Serve an important bridging role" by facilitating academic exchanges and formal partnership agreements between NOAA and the PRC institutions at which the subject held concurrent positions, thus representing both parties during negotiations and violating US government ethics rules.

Clearly, most of these activities undermine the basic values of research integrity. Another highly disturbing element was discovered when federal investigators interviewed at least one of the PRC national researchers the subject hired. At least one of these PRC nationals stated that the NOAA researcher pressured him or her to work exceedingly long hours in the lab: they had to sleep and work in the lab on the weekends and do the lion's share of the research and drafting of publications that the NOAA researcher would claim as his own. The NOAA researcher exploited a power dynamic where the PRC nationals needed positive performance reviews for their careers back in China; if they complained to NOAA management, the NOAA researcher would take retaliatory measures against those PRC nationals.

Other investigations I supported involving talent program selectees at US academic institutions resulted in similar findings. Many part-time talent program selectees (those that retain their US positions) are tasked by their PRC employers or party-state organs to hire or sponsor specific PRC national PhD students and postdocs to work at US institutions to gain access to and support the research done there. Many of these talent program selectees were PIs on federal grants. Investigations also discovered that some of these US faculty members who were talent program selectees coordinated with the China Scholarship Council to provide funding for the PRC graduate students and postdocs' study in the US. A few of these cases *also found abuse and exploitation of the PRC national students, unbeknownst to the US institution.*

Academia has argued that recruiting individuals from personal and professional networks is a normal practice. However, it is important to differentiate this from the activity I am describing, which involves direct taskings - often under contractual obligations - by the PRC government to sponsor specific individuals and ignore standard, merit-based hiring practices. At a minimum, this undermines the integrity of our open system; it is more damaging when individuals carry out research projects conducted by specific individuals at the behest of the PRC party-state in critical technology fields.

We do not know the scale or scope of this phenomenon. Nevertheless, when we examined numerous talent program selectees in prominent positions at US universities who are PIs on federal research grants, it was not uncommon to find that the majority of their graduate student body are PRC nationals, typically from select (and often high-risk) PRC institutions with which these faculty members have formal relationships via PRC talent recruitment programs. This calls into question oft-used arguments that there is insufficient US and other allied nation STEM talent available to fill graduate degree and postdoctoral programs at US universities or laboratories and that we are critically dependent on PRC talent. When some US faculty are financially obligated by their overseas (PRC institution) sponsors to appoint personnel, domestic STEM talent is simply overlooked or a lower priority. This practice has

been observed to take place for two decades, making this "dependency" on PRC talent highly concerning and a self-fulfilling prophecy.

Case Example 2: Former UCLA Professor

While in government, I also supported efforts that identified then-UCLA Professor Songchun ZHU as part of a larger survey of US-China collaboration on AI and computer vision disciplines. We looked closely at Professor ZHU because of his extensive partnerships with PRC entities that represent national security, integrity, and grant compliance concerns. ZHU had worked on DoD and NSF-funded research totaling over $30 million while simultaneously having significant commitments with PRC organizations, including via China's flagship Thousand Talents Program. In addition to suspected disclosure failures of current and pending support on grant applications, ZHU appeared to divert federally funded research to private companies he founded and ran (based in China and the US). In other words, he was commercializing federally funded research for personal (and arguably China's) benefit.

ZHU also partnered with and had talent program appointments at the Beijing Institute of Technology (BIT) and other PRC research institutions heavily involved in defense R&D. BIT is a "Seven Sons of National Defense' university involved in weapons and defense program research. Even if he was not violating US law, his PRC collaborations and appointments represented serious national security and conflicts of interest and commitment concerns.

In 2019, I provided extensive information on ZHU to DoD law enforcement and intelligence components as well as senior DoD leadership to demonstrate the nature of these threats. No actions appear to have been taken, at least while I was in government. ZHU recently relocated to China and now leads a massive AI research effort there, as reported by *Newsweek.*[24] The decades of knowledge and research projects he conducted for DoD are presumably furthering China's AI efforts, including in applied domains through his companies. Many of the PhDs and postdocs he sponsored and trained at UCLA subsequently worked at his companies. Some of those individuals are now in China, leading major AI, computer vision, and related research that have mass surveillance and military applications. The US taxpayer, especially through DoD funding, trained multiple generations of PRC scientists in critical technology fields who are now at institutions supporting PRC military and public security organs.

Case Example 3: Influence Over NSF Grant Award Processes

NSF relies heavily on Intergovernmental Personnel Act (IPA) assignees, typically academics in scientific and engineering fields, to take temporary assignments to serve as program directors and grant managers. These individuals oversee NSF grant application submissions, evaluation and award processes, and related grant program management functions. IPAs

[24] Didi Kirsten Tatlow, "Exclusive: U.S. Gave $30 Million to Top Chinese Scientist Leading China's AI 'Race'," *Newsweek,* November 1, 2023, https://www.newsweek.com/us-gave-30-million-top-chinese-scientist-leading-chinas-ai-race-1837772.

are not federal employees but are subject to provisions of law governing the ethics and conduct of federal employees.[25]

While in government, as part of my interagency efforts to assess risks and threats associated with PRC talent programs, my colleagues and I discovered a troubling issue: some talent program selectees who were faculty at US universities took IPA assignments at NSF to serve as grant managers. We compiled data on the NSF grants that those individuals were responsible for (which included making grant award decisions) and found that some of the grants were awarded to researchers who were also selectees of the same PRC talent programs. Additionally, several of the awardees (PIs) of these NSF grants who were recruited by PRC talent programs subsequently became IPAs at NSF themselves and then awarded grants to *other* PIs who were PRC talent program selectees and to former IPAs. One of the talent programs that all of the identified IPAs were affiliated with was established around the year 2000; the first IPA position of one of these talent program selectees began around 2005.

Consequently, we observed a vector of influence where individuals simultaneously under contract with the PRC government were making NSF grant award decisions for two decades. The number of individuals we found implicated in this scheme was small. However, due to limited resources, our focus was only on one NSF division. We do not know whether this type of activity has taken place at other NSF divisions. Additionally, *I am not aware of any efforts since that discovery to identify similar activity at other federal agencies that employ academics (typically as IPAs) as part of their grant management structure.* This is just one method of the PRC's malign influence over federally funded research.[26] Based on my experience, it appears that the scale and scope of PRC influence activities over federal grant award decisions are largely unknown.

Exploitation of Other Federal Funding Sources

Hijacking NSF CAREER Awards

The PRC government clearly prioritizes the recruitment of individuals who received or supported federal research grants. PIs on DoD grants are obviously of very high interest for China to recruit, but talent programs have also recruited many recipients of other agency funding. A troubling trend is China's recruitment of academics who recently completed or are nearing completion of their term as an NSF CAREER awardee. "The Faculty Early Career Development (CAREER) Program is a Foundation-wide activity that offers NSF's most prestigious awards in support of early-career faculty who have the potential to serve as academic role models in research and education and to lead advances in the mission of

[25] https://new.nsf.gov/careers/rotator-programs/intergovernmental-personnel-act-ipa-assignments
[26] NIH has discovered and disclosed publicly a situation where the confidential peer review process of grant applications was compromised by some PRC-affiliated actors. This represents a similar type of influence, but it is not known how pervasive this activity is.

their department or organization. Activities pursued by early-career faculty should build a firm foundation for a lifetime of leadership in integrating education and research."[27]

In other words, NSF's CAREER program is an investment in future science and engineering leaders, where they are given a prestigious line of funding to kickstart their promising and lengthy careers in the US. PRC talent programs have been observed to recruit some of these individuals to work in China, *thus benefitting from (and exploiting) the significant investments made by the US government and further eroding our STEM talent pipeline.*

Exploiting SBIR Programs

PRC talent programs have also targeted recipients of DoD-funded Small Business Innovation Research (SBIR) programs. A small (government-use only) study I supported while I served in government found that China has benefited from DoD's SBIR programs and revealed vulnerabilities to potential future DoD supply chains. Not all of China's exploitation of SBIR contracts involved the use of talent programs, but in many observed cases, key personnel (founders, chief scientists or engineers, CEOs, etc) of startups receiving SBIR funds were recruited through a talent program or received PRC state-backed start-up capital.

- Some key employees of US firms receiving SBIR contracts were recruited via a PRC talent program and relocated to China, but they continued research collaboration with officers of the US companies where they were previously employed.

- US firms established PRC-based subsidiaries, receiving funding through entrepreneurial contests that function similarly to talent programs. In some cases, the firms subsequently dissolved their US operations.

- In one observed case, a recipient of multiple DoD SBIR contracts established another firm in China based on the same technologies, developing combat vehicles in partnership with the state-owned defense conglomerate China North Industries Group Corporation (NORINCO).

Technology Acquisition Networks

There are organizations in the US (and around the developed world) that demonstrably partner with, take tasking and direction from, or serve as a proxy to CCP organs and the PRC diplomatic missions. In the US, these entities are typically non-profit professional associations that claim to be NGOs. While many of these organizations engage in professional networking and entrepreneurial activities that are not illicit in nature, they have supported PRC state-directed activities, *including substantial involvement with PRC talent programs*. Details on specific organizations and case examples cannot be provided in this testimony, as the preparation and dissemination of the information is considered government use only.[28] However, I can offer some key findings:

---

[27] https://new.nsf.gov/funding/opportunities/career-faculty-early-career-development-program

[28] Note however, that some organizations, particularly those principally engaged in technology transfer activities, are described in the edited volume, *China's Quest for Foreign Technology: Beyond Espionage,* Hannas and Tatlow eds., Routledge, 2021)

- Key leadership of some of these non-profit organizations are federal government researchers at NOAA, NASA, the Department of Energy, etc. Yet these organizations routinely meet with and receive taskings from CCP organs and PRC diplomats (especially in the S&T and Education sections of the PRC Embassy and its consulates).

- Some organizations organize, host, and serve as judges for talent programs and start-up contest activities operated or sponsored by the PRC government. The leadership of these organizations runs venture capital and angel investment structures in the US.

- Some of these organizations also routinely meet with (and likely take instruction from) CCP United Front organs and PRC diplomatic mission personnel in the US.

One organization that is publicly known to have overseas operations and closely partner with (i.e., task) diaspora organizations is the Western Returned Scholars Association (欧美同学会 - 留学人员联谊会, WRSA). WRSA is a CCP organ directly subordinate to the United Front Work Department, described as "a mass organization led by the CCP, composed mainly of returned overseas scholars, [serving as] a bridge and link between the Party and the vast majority of overseas scholars, helping the Party and state do overseas scholar work well, [and acting as] a home for the vast majority of overseas scholars."[29] WRSA has been observed to partner extensively with some of the non-profit organizations I described above.

III. China's Role in Undermining Research Integrity and US Inaction

Research security, research integrity, and malign influence are often intertwined, especially when dealing with the PRC. Governments and research institutions in liberal democracies espouse and stress the importance of values such as academic freedom, transparency, integrity, and reciprocity concerning the conduct of research and international research collaboration. The G7 Security and Integrity of the Global Research Ecosystem Working Group defined a set of "Common Values of Research Integrity," which included transparency concerning disclosures of researcher affiliations, conflicts of interests, and sources of funding, and honesty regarding proposing, undertaking, reviewing, and communicating research.[30] However, **PRC party-state organs and research institutions routinely violate these norms and values that are critical to beneficial research collaboration and trust in science**.

Research organizations in liberal democracies rarely take transparency and integrity factors into account when engaging with the PRC. When allied nations, especially G7 countries, espouse "common values" of transparency, integrity, and reciprocity but impose no cost to Chinese researchers and institutions that violate these values, they signal to PRC entities that the status quo is acceptable. *The US government has taken no observable policy*

[29] The original source is no longer available online; an archived version can be found here: https://web.archive.org/web/20190802122850/http://www.xinhuanet.com/politics/2016-08/03/c_1119332162.htm.
[30] "G7 Best Practices for Secure & Open Research," Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, May 2023.

measures to mitigate PRC practices that undermine research integrity, and these practices are often intended to influence the international research community.

My non-profit's latest publication catalogs numerous ways China has violated these norms and the implications of academia and government inaction.[31] My colleagues and I examine China's lack of transparency, which often is intentional to mislead the international community, as well as types of fraud in published scientific literature. Academic fraud in publications is a global phenomenon and by no means unique to China. However, China is by far the world's largest producer of fraudulent publications, which has a profound impact on trust in the global research enterprise.

As Glenn Tiffert writes in the foreword of my publication, "The party has grown less tolerant of open inquiry, debate, and free flows of information…It controls knowledge at home with the most sophisticated regime of propaganda, surveillance, and censorship on the planet, and abroad by cutting off foreign access to PRC scientific, judicial, and economic information, and to the academic theses and journals that nourish independent judgments. It is securitizing data and has recriminalized forms of collection and analysis that are routine in open societies."

The issues Tiffert describes should warrant rigorous policy responses from both governments and academia, yet the silence is deafening. The incentives and interests of individuals and their research institutions probably drive inaction. Research institutions routinely make exceptions to their espoused values and core principles of academic research when dealing with China. Examples of China's practices include:

- Adding foreign coauthors who had no material involvement in the research to bolster the reputations of the other coauthors and institutions
- Listing a PRC institution as the only affiliation when most or all of the research occurred outside of China
- Creating fictitious coauthors with stated affiliations to reputable foreign institutions
- Producing fake papers in paper mills; intentionally using falsified or manipulated images or data
- Denying access to PRC websites of institutions from outside China or removal of content
- Obfuscating or misrepresenting PRC entity names, missions, projects or funding sources, parent organizations, etc.; discrepancies between English and Chinese information that strongly suggest intentional deception
- Failing to disclose financial conflicts of interest or outside involvement (as a shareholder, company board member, founder or chief scientist/engineer of commercial firms) on any CV, faculty page, or (co)authored publication

[31] Stoff, McIntosh, and Lee, "Transparency and Integrity Risks in China's Research Ecosystem: A Primer and Call to Action," *Center for Research Security & Integrity*, 2024.

For-profit academic journal publishing firms have few incentives to self-police and systematically identify and retract fraudulent papers. The journal industry earns money from paper mills, and retracting papers is a burdensome process. It is assumed that a substantial number of fraudulent publications remain undetected (not retracted) and continue to be cited. Outside of publishers, monitoring to detect fraudulent research and publications is largely limited to voluntary and often self-funded efforts by a disturbingly small international community of individuals, many of whom contribute to PubPeer.com and Retraction Watch.

PRC entities that lack transparency or integrity undermine trust, complicate due diligence and risk assessment efforts, and create an unsecured research environment. Fraudulent publications can be harmful when scientists, clinicians, or even policymakers make decisions based on fake or manipulated science.

Case Example: 'Comfort Letters'

I advised on other investigations when I was in government – some of which involved instances where a PRC institution provided a letter to NIH that contained demonstrably false information to mislead a grant compliance investigation. The cases involved PIs at US research institutions under investigation for allegations of failure to disclose outside appointments or affiliations with a PRC institution. In a few cases I supported, the PIs were assigned to work 12 months per year on a federal grant; thus, undisclosed appointments may represent conflicts of commitment and violate NIH grant terms.

NIH posted an illustrative case on its website. A Senior Deputy Director of Research at a PRC university provided an official "comfort letter" (as NIH describes it) to the scientist and the US institution, stating that the scientist under investigation was merely honorably invited as a guest professor, did not hold any official faculty position, and had no formal contract through a PRC state-run talent program; the individual just had a "gentlemen's agreement" with the PRC entity. However, the employing US institution reported to NIH that it discovered documents indicating the researcher did, in fact, receive a talent program position and had a formal agreement with the foreign university to work as a "distinguished part-time professor" for three years.[32]

This "comfort letter" provided to the US institution was intended to deny and deceive NIH, and having it sent by a senior leader from a PRC institution indicates institutional-level dishonesty. NIH has received an undisclosed number of "comfort letters" from PRC research institutions. Thus, it is not known how many PRC institutions were involved or how pervasive this dishonesty has been. Regardless, this problem calls into question whether US researchers should receive federal research funding on projects that involve collaborations with PRC entities that have sent false and misleading information to federal agencies. I am not aware of any policy at federal funding agencies that addresses this issue. *Consequently, neither the US employing institution nor the federal agencies are imposing any costs to this*

[32] Posted case studies are available on the Policy and Compliance page of the NIH website: https://grants.nih.gov/policy/foreign-interference/case-studies.

behavior, despite it fundamentally violating academia's core principles and "common values."

Reciprocity

Issues of reciprocity are also not receiving scrutiny, and government and academia's inaction raises important policy questions. Here are two examples:

US-China research collaboration also takes place at federal agencies via national laboratories, federal facilities, and other government-run infrastructures that carry out their own research. Some of these agencies oversee collaborative projects with the PRC through formal agreements. When I was in the government, officials at several federal agencies discussed the fact that sometimes, the partnering PRC institutions failed to abide by the terms of a research agreement, such as failing to provide the promised resources, data, or personnel. In some cases, an agency decided to cease or not renew such a partnership. In other cases, collaborations continued despite the PRC not meeting its obligations - perhaps in the interest of furthering diplomacy or gaining cooperation from the PRC in other areas.

Similarly, PRC data/information laws can restrict or prohibit PRC research institutions from sharing the underlying data on published research with the rest of the world. When findings are published based on data, but the PRC prohibits its release, then the research community cannot validate or replicate the research results or methods elsewhere. I have seen very little investigation or scholarship on when and how often this occurs, whether federal research funding was involved, or whether the US government has developed any policy response.

IV. Brief Discussion of IC, FBI Failures, Knowledge Gaps

The introduction section listed some of the shortcomings that hamper the Intelligence Community (IC) and law enforcement (particularly the FBI) efforts to protect our research and innovation ecosystem. This issue is too complex to examine comprehensively here, nor is this the focus of the hearing. *However, there are areas worth noting that relate to the government's (in)ability to identify and disrupt the PRC's malign foreign influence activities in the US.*

There has been an observable decline in researching, investigating, and mitigating the threats posed by PRC talent programs due to unforced errors by the FBI and the Justice Department. Execution of the "China Initiative" led to a reckless focus on attempting to arrest and prosecute selectees of PRC talent programs in academia. The US government had to learn a painful lesson: criminal statutes often do not apply to fundamental research activities in academia. The failures resulted in a backlash within academia and the Asian-American community in particular, who justifiably felt unfairly targeted and, in some cases, severely disrupted the careers of academics.

When I was in government, there were a few individuals (including me) who unsuccessfully tried to convince agencies to focus their resources on leveraging civil, administrative, and other tools and tactics to mitigate the threats rather than pursue prosecutions. Offices of

Inspectors General began pursuing civil investigations and remedies, but those efforts were nascent, and a lack of sufficient expertise limited their scope.

To be fair, the FBI *successfully prosecuted* several important cases involving economic espionage and IP theft, some of which involved talent programs. I would be remiss not to underscore the fact that PRC talent program selectees can be tasked or incentivized to steal materials, data, and IP, and provide false statements or claims to the federal government that can be illicit in nature. Much of these activities are not limited to targeting or exploiting academia; the private sector has been affected, but there is even less public knowledge about the scale and scope of that malign activity because capital markets (and shareholders) do not look kindly on public companies that are victims of technology theft. Nevertheless, a consequence of the FBI's failures is that there has been little space for nuanced discussions of the insidious nature of many of China's talent programs, including aspects that go beyond the national and economic security concerns discussed in this testimony.

Another key impediment of the IC is the paradox of mission priorities. The early stages of our research and innovation ecosystem have, by design, the least amount of regulatory oversight. This lack of oversight has meant a lack of resources or mission priority within the national security community to protect these areas. That has left our ecosystem largely unprotected from China's predations, which, unsurprisingly, China has increasingly exploited.

Additionally, the IC's continued descoping and devaluation of open-source intelligence (OSINT) and diminishing use and reliance on publicly available data sources and information further degrades the government's ability to protect academia and private sector entities. This has led to persistent and yawning knowledge gaps in the PRC's research ecosystem that pose strategic risks and is one cause of the dearth of subject matter expertise on China's technology transfer apparatus.

The IC cannot be trusted to collect and provide OSINT, especially data collection and analysis that can support institutions outside of the government. This is not as controversial as it seems; numerous studies by think tanks, policy papers, etc., have advocated radical changes to the process and prioritization of OSINT activities of the US government. Yet variations of these recommendations started in earnest after 9/11, and the same conversations have continued with no meaningful change in structure, mission priorities, or budget.

Part of this problem is structural and bureaucratic: SIGINT, HUMINT, and other technical collection means are sophisticated and expensive, and the IC places a much higher premium on clandestinely acquired information than publicly available information. OSINT elements of the IC, particularly the CIA, have been gradually descoped and underfunded. Leadership considers the OSINT profession second-class, where expertise is devalued, and career progressions of officers are limited. I do not foresee any real change to this situation.

As an example, when I was in government, I oversaw several pilot open-source projects that built databases and related repositories of information on China's research ecosystem, especially elements of China's defense research and industrial base. As the information was derived from public sources, the intent was to make the information available broadly to federal agencies, scientific funding agencies, the State Department, the Department of Homeland Security (DHS), and export and financial regulatory bodies. All of these projects were ultimately discontinued, and the information has largely remained in silos within the IC. These efforts were not a mission priority.

I also provided information to counterintelligence elements on organizations that have demonstrable ties and partnerships with CCP organs, the PRC diplomatic establishment, and PRC state-backed investment structures. Little action was taken (at least while I was in government). My interactions with FBI and DoD counterintelligence elements showed that those offices prioritized criminal investigations over leveraging operational approaches to deny and disrupt PRC state-directed technology transfer and related influence activities.

Persistent Knowledge Gaps

Research institutions and federal agencies will continue to be ineffective at identifying and mitigating risks associated with research partnerships with PRC entities as long as yawning knowledge gaps persist. Some examples follow.

China's Defense and Surveillance Research and Industrial Bases

Areas where there is little information nor any systematic efforts to collect such information include:

- A knowledge base (such as lists and descriptions) of all subsidiaries of PRC state-owned defense conglomerates that house research institutes and conduct defense R&D or sponsor academic research
- Identification and assessment of national and provincial-level key laboratories' and Chinese Academy of Sciences institutes' level of involvement in defense (or classified) research and their partnerships with the PLA, defense industries, and civilian universities principally engaged in defense research
- A knowledge base on PRC universities that have substantial ownership stakes in companies supplying the PLA, defense conglomerates, or public security organs
- A knowledge base on PRC universities that conduct research with mass surveillance applications or other disciplines enabling human rights abuses and/or receive funding from PRC public security organs
- Identification of PRC research centers of excellence that are domestic leaders in fields the US government has designated as critical and emerging technologies, such as AI, quantum computing, certain biotech fields, and semiconductors

University-Industry Integration

There is also insufficient knowledge on how PRC research institutions integrate with or support domestic industries. Integration occurs in a myriad of ways, yet there is little scholarship on the subject. I am also not aware of any efforts to systematically examine these topics by federal agencies. Examples of topics include (but not limited to):

- Some universities are co-managed by or have partnership agreements with state-owned enterprises, where students and faculty directly support commercialization efforts and train future technicians for those enterprises. Beijing University of Chemical Technology (BUCT), for example, is a top chemical engineering school that is partially overseen by Sinopec (one of China's state-owned oil giants). BUCT conducts research on behalf of this large state-owned firm and the two entities share some personnel.

- Some professors at research institutions concurrently serve as scientists, engineers, and/or founders of technology firms while enjoying extensive international R&D collaborations in their academic capacity, raising the risk of unknown technology or knowledge transfers that solely benefit PRC enterprises.

- Some PRC universities and Chinese Academy of Sciences entities have majority or substantial ownership stakes in dozens, if not hundreds of commercial enterprises. This is often opaque to the international community. A report by US-based non-profit C4ADS examined corporate records of the Harbin Institute of Technology and found that the school has direct or indirect ownership interests in approximately 1,000 China-based companies and owns a 50 percent or greater ownership interest in about 50 entities.[33]

- PRC commercial sector interests and ties to academia may influence the research or content of publications; how and to what extent does the PRC use academic research as an instrument of its industrial policy.

V. Brief Overview of Allied Nations and Innovation Security

Despite my frequent criticisms of US government in this testimony, I would be remiss not to recognize that many federal agencies have led the international community in raising awareness of the risks and threats the PRC poses to our collective research ecosystems and have made great efforts in promoting research security. Our key allies and partners are becoming increasingly aware and concerned with research security and integrity concerns thanks in no small part to the US government. That said, government efforts to date have been mostly limited to raising awareness of current problems and challenges, and it has been less effective when it comes to mitigating and reducing the threats, especially within fundamental research domains that are subject to less oversight in liberal democracies.

Key allies have investigated and discovered similar threats posed by China to those encountered by the US. An infamous example is the case of a Canadian scientist who was

[33] Jason Arterburn, "The Party-State in China's Military-Industrial Complex: Implications for U.S. National Security," Testimony to the U.S. - China Economic Security Review Commission, March 19, 2021, https://www.uscc.gov/sites/default/files/2021-03/Jason_Arterburn_Testimony.pdf.

fired from her position at a level-four virology lab due to allegations of misconduct and national security concerns associated with her collaborations with PRC institutions, including military medical entities.[34] Another case involved a Beihang University student funded by the China Scholarship Council to study in France, who repeatedly accessed laboratory computers using other students' credentials, a clear violation of the IT policy. The student also stayed overnight in the laboratories and facilitated unauthorized access for a compatriot who had no official business in the lab. This individual reportedly used laboratory equipment, potentially for unknown purposes.[35]

Many EU governments appear to take a "country agnostic" approach to research security to avoid the appearance of having discriminatory policies. It is true that many policy mechanisms to mitigate risks can be framed more broadly – that our standards, values, and restrictions are not country-specific, especially concerning authoritarian and adversarial regimes. Nevertheless, the uncomfortable reality is that probably over 90% of all the threats and challenges to our collective research ecosystem come from the PRC. Within the EU, for example, nearly all partnerships and research collaborations with Russia have stopped due to its invasion of Ukraine. And several EU nations have discussed the need to build better competencies on China (i.e., subject matter expertise).

Having 27 individual member states in the EU creates inconsistencies in how research security is approached across the region, with some states having more robust measures in place while others may have a higher tolerance for risk and/or lack of capabilities to address their vulnerabilities. An absence of centralized oversight in the EU also allows China to engage in partnerships or research activities with less oversight or scrutiny.

My direct engagements with foreign partners have been limited to a few EU nations; as such, I cannot provide a comprehensive view of the current research security landscape across all of our key allies and partners. Instead, I offer some observations based on personal interactions with government organs and research institution leaders.

I have engaged the most with Germany and The Netherlands, and their governments have been active in raising awareness and addressing issues on research security, including providing concrete guidelines and recommendations for academia. There are more open discussions (and recognition) of the concerns related to China's unilateral knowledge transfers, malign influence - especially when it impinges on academic freedom, and diversion of research that enables human rights abuses or supports the PLA.

The Netherlands appears to have the most well-developed set of policies and programs on research security among EU member states, based on my observations. The Dutch government has created a "national contact point" - an office where research institutions can request due diligence and risk assessment support (especially on China) regarding any

---

[34] See for example: https://www.cbc.ca/news/canada/manitoba/scientists-fired-from-winnipeg-lab-rightly-under-probe-1.7150560 and https://www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7128865.
[35] https://www.mediapart.fr/journal/france/140222/une-etudiante-chinoise-espionnait-des-laboratoires-francais) Clément Le Foll et Matthieu Suc, Feb. 14, 2022.

partnerships they are pursuing. However, there is still a need to build Chinese language and subject matter expertise even in the Dutch government, to be more effective in providing support. That said, partly due to the small number of universities in the Netherlands, there appears to be a close-knit research security and compliance community that is exploring ways to share information among and between them and is well aware of the PRC's malign influence risks. The Dutch also appear to be a valued and contributing partner to the international innovation security community.

Germany is much more active compared to just a few years ago in raising awareness and deliberating on policies on research security. Yet, many challenges remain. Generally speaking, Germany, like the US, is mentally and politically ill-equipped to deal with the malign influence and threats posed by China, partly because there is a general lack of understanding of the *systemic, networked nature of China's strategy*. Problem areas are viewed as "individual cases" within academia. (I have heard similar arguments in the US.)

German sinologists Alicia Hennig and Andreas Fulda recently opined that German policies still leave critical "blind spots" that need addressing. For instance, they argued that "reciprocity is not achievable with regard to Chinese laws" and that the German side "still assumes that access to and use of information from joint research projects can be secured through framework conditions to its own advantage."[36]

While there is an observable decline in Sino-German institutional cooperation, PRC national students continue to flow into Germany in very large numbers. Many of them start at undergraduate and Master's levels, which limits federal government oversight. However, this serves as a gateway for individuals to stay in Germany and further advance to PhD, postdoctoral, and higher levels within academia, many of whom focus exclusively on critical technologies. However, commercial spinoffs and other entrepreneurial endeavors of individuals earning PhDs and postdoc positions are rarely founded by PRC nationals. Many return to China after gaining the critical knowhow to launch enterprises there.

Another challenge Germans have articulated relates to a lack of reciprocity, which is also not unique to the German experience. Thousands of PRC students go to Germany every year, but almost no Germans go to China because critical technology disciplines are taught exclusively in Chinese. Worse still, PRC nationals have unfettered access to German equipment, data, algorithms, and supercomputers; however, in China, the PRC government considers these strategic assets to be mostly closed to foreigners.

German professors are civil servants with employment protections and few incentives or pressures to commercialize their research. The PRC takes largely an opposite approach. Academic freedoms and the system Germans operate in create no incentives to cut ties with China, especially when allied nations share the same view or the US chooses not to apply

[36] Hennig and Fulda, "Blind spots in scientific cooperation with China," *Table.Media*, January 14, 2025, https://table.media/en/china/opinion/blind-spots-in-scientific-cooperation-with-china/

pressure on restricting PRC collaborations. Unfortunately, the current political climate in the US is also driving many German scientists to prefer working with the PRC rather than the US.

Another common theme I have encountered is that EU-based professors become increasingly reliant on PRC young talent if they cannot find sufficient STEM talent from the US and other friendly nations. Germany, and especially smaller nations like The Netherlands and Denmark, have world-class scientific institutions but rely heavily on large international student bodies. This creates more student mobility opportunities (especially at graduate degrees) for the US and would be welcomed by our EU partners.

VI. Recommendations for Policy Makers

The challenges we face in mitigating and disrupting the PRC's malign influence and exploitation of our research ecosystem are daunting. However, the following recommendations, if implemented, would go a long way in closing regulatory and knowledge gaps, re-aligning incentives and grant compliance of academia, limiting the PRC's near unfettered access to federally funded research, and leading the international community to ensure the integrity of research is not an abstract construct – that real costs are imposed on the PRC when it violates commonly accepted norms and values.

Many of these recommendations go beyond the remit of the Senate Foreign Relations Committee. The challenges and threats posed by the PRC transcend the missions of individual agencies and legislative committees. We must find the courage to aggressively break down silos and partisan barriers and build new paradigms for cooperation among and between federal agencies and legislative committees. Otherwise, our fragmented and piecemeal measures will not be able to stand up to China's whole-of-society approaches.

It is worth noting that my recommendations *exclude* much-needed efforts to bolster domestic STEM research and education to reduce dependencies on adversarial nations like China. Research security is pointless if we lose the technology at the point it is ready to leave the lab because we lack the ability to manufacture it competitively or an engineering workforce and risk capital to support pilot projects and work through scaling challenges. We have allowed many of the links in the chain to atrophy by outsourcing so much of our inputs, including human capital. However, as we bolster domestic investments in R&D, we need a corresponding increase in protection and research security policies and measures, especially given the current abysmal state of neglect by both the government and academia.

My recommendations include a) bolstering research grant compliance and enforcement by federal agencies; b) enhancing disclosure laws and policies; c) improving the State Department's visa vetting processes; and d) through State Department leadership and interagency cooperation, build programs, infrastructures, and policies exclusively dedicated to research security **and** integrity. These recommendations are not presented in any hierarchical order in terms of priority; I start with listing recommendations that involve the State Department and are most relevant to this Committee's oversight functions.

1. **Enact new legislation similar to the requirements of Section 117 of the Higher Education Act for the purposes of reporting information to the State Department.**

Similar to the current requirements of reporting foreign contracts, gifts, and grants to the US Department of Education, institutions of higher education and other research organizations (such as hospitals and medical research facilities) should be required to report to the State Department all MOUs, cooperative agreements, joint degree programs, joint venture educational institutes based overseas, and other related agreements with foreign countries of concern. "Foreign countries of concern" are determined by Congress and should be consistent with other legislation (which usually names Russia, Iran, the PRC, and Cuba). Information should include details on the foreign entities (and their subdivisions) that are

counterparties to the agreements; the periods of performance or length of the agreements; and a listing of responsible persons overseeing the execution of the agreements. State Department should create a dedicated repository of this information that is made available to all law enforcement agencies (FBI and Offices of Inspectors Generals), DHS, the Intelligence Community, and federal agencies that provide research funding to higher education institutions.

Additionally, US institutions that sponsor foreign nationals for PhD, postdoctoral, or visiting researcher positions should be required to include in their invitation letters that accompany the visa applications of the foreign nationals indications that the invitations are part of a formal MOU, cooperative agreement, joint training program, etc.

2. Amend the Foreign Agent Registration Act (FARA) to expand the definition of an "agent of a foreign principal."

The Department of Justice has recently sought public comment on proposing some amendments to FARA regarding the scope of certain exemptions, to update and add various definitions, and other implementing regulations. However, a cursory examination of these proposed changes suggests key elements of the rules would remain intact: the scope of FARA is largely limited to political activities - purely commercial and academic pursuits are exempt from current FARA regulations. FARA needs to evolve with the changing geopolitical landscape, particularly concerning PRC influence activities in the US.

All selectees of any PRC state-sponsored talent program, which includes programs run by national, provincial, and municipal level party-state organs, should be required to register as agents of a foreign principal. This holds true even if the selectees are academics. All PRC talent program selectees are under contract with / employed by the PRC government, subject to PRC laws, and receive tasking and direction from the PRC government to pursue the PRC's strategic objectives, which invariably harm US interests. While the act of being a selectee of a PRC talent program is in itself not illegal, individual selectees should be registered foreign agents. Failure to register under FARA should result in criminal penalties or, in the case of foreign nationals, visa revocation and deportation.

Similarly, entities incorporated in the US, including non-profit organizations and associations, that execute the duties of or receive taskings or monetary support from PRC party-state organs (including but not limited to PRC diplomatic missions) should also be required to register as foreign agents. China has exploited loopholes in FARA by deploying proxy organizations that, while claiming to focus only on academic, educational, or commercial pursuits, are, in fact, executing state-directed and sponsored technology acquisition efforts, political lobbying and policy advisory activities, and support functions to PRC public security organs including serving as overseas "police stations."

3. Improve the State Department's visa information storage systems and sharing processes and bolster enforcement of current visa restrictions.

Consular offices face huge resource constraints in terms of due diligence and vetting of PRC nationals on visa applications, given the sheer numbers involved. Improvements in IT

systems and processes regarding visa applications would allow for more interagency support - especially from DHS - that assists with the Security Advisory Opinions (SAO) process for visas that require security background checks on applicants. PhD students, postdocs, and other visiting scholar applications (usually on F and J visas) include supplemental information such as an applicant's CV or resume, invitation letters from the sponsoring US institution, and other supporting documents. It is my understanding that most of these supporting documents are manually scanned as images, losing the original file formats. Consequently, none of this supporting documentation attached to visa records can be indexed, searched, or retrieved by DHS or other national security agencies for risk identification or inputs into the SAO or related processes.

Congress should appropriate funding for the State Department to modernize its information system storage and retrieval infrastructure that allows for the retention of original file formats (such as requiring electronic submissions) and a process for indexing all information contained in visa applications that can be searched and retrieved through automated processes and incorporated into other internal government databases as appropriate.

The State Department should also expand the scope of organizations that would be included in visa denials in accordance with Presidential Proclamation 10043 of May 29, 2020. This proclamation is intended to deny certain student visas (limited to PhD students and postdoctoral applicants) if they are affiliated with any entity that supports the PRC's "military-civil fusion strategy"; that strategy is defined as any actions "to acquire and divert foreign technologies, specifically critical and emerging technologies, to incorporate into and advance the PRC's military capabilities."[37] Knowledge gaps and varied interpretations of what entities constitute support to "military-civil fusion" have limited the effectiveness and enforcement of this rule.

In the short term, an easy (partial) solution to this problem is to simply include in this proclamation all PRC entities already listed on the various US government restricted lists. Specifically, visa denials should be applied to any individual employed at or affiliated with entities on the BIS Entity List, Treasury's OFAC sanctions list, and organizations listed based on the provisions of Sections 1286 and 1260H of the National Defense Authorization Act. These lists are by no means exhaustive and need to be updated. Nevertheless, the US government has already determined that entities on these various lists pose significant national security threats and should thus form the basis for visa denials outlined in Proclamation 10043.

4. **Create a new office in the State Department focused exclusively on technology transfer, research security, and research integrity issues. This office, nominally referred to here as the Office of Innovation Security and Integrity (OISI), should develop new policies and programs and coordinate/expand on existing department-wide efforts.**

[37] https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic

Regional bureaus, public diplomacy elements, and the Bureau of International Security and Nonproliferation currently oversee programs and international engagements that deal with research security and technology transfer to some extent. However, these efforts sometimes lack coordinated, strategic approaches. Additionally, while the State Department has received additional funding for and actively engages in efforts to counter China's predations in a variety of areas, there are still important elements that are missing or receive inadequate attention. In addition to policy development and coordination functions, this new Office of Innovation Security and Integrity[38] should carry out (but not be limited to) the following lines of effort:

A. Lead the international community in greatly expanding knowledge and capacity building (i.e., competency) on China relating to research and innovation security.

This testimony has highlighted many knowledge gaps on PRC entities and programs of concern regarding its research ecosystem and technology transfer apparatus, which I attribute mostly to failures of the IC. State Department should take a leading role in this space, leveraging a variety of public and private sector institutions and the international community in the following areas.

Oversee the creation of a new version of the existing "China Defense Universities Tracker" created by the Australian Strategic Policy Institute (ASPI).[39] This is a web-based repository of information on select PRC universities and research institutions tied to China's military and defense industries and has been wildly successful in terms of its use around the world. Most research security and compliance offices have leveraged this tool extensively to support due diligence efforts. However, this web-based tool is quite limited in scope. For example, it has not been updated, nor does it comprehensively identify all research institutions or their subdivisions and laboratories that conduct defense research. The tracker also has minimal information on research institutes attached to defense state-owned enterprises and contains no information on Chinese Academy of Sciences institutes (which number over 100).

State Department's new "OISI" should replicate this effort but significantly broaden the scope to address the ASPI tracker's limitations. The tool should also be made available publicly to assist the international research community. OISI should also replicate this model to build other information repositories, as discussed below.

Sponsor and/or oversee additional international research collaboration projects that expand the knowledge base on China's research ecosystem, starting with projects on identifying PRC centers of excellence in critical technology R&D areas.

OISI should develop programs that build a consortium of organizations that collaborate on research projects. Projects should tap into experts and organizations across the EU, Five Eyes, and Indo-Pacific allies, such as experts in particular critical technology disciplines in academia, think tank scholars and NGOs, private sector data providers, and other

[38] This is simply a placeholder name; Congress and State Department can create an appropriate title for this office.
[39] https://unitracker.aspi.org.au/

organizations that can collaborate on methods and studies that identify PRC technology centers of R&D excellence: the research institutions, labs, key personnel, supporting infrastructures, etc. These efforts can include technical evaluations of research conducted in the PRC, surveys of domestic and international partnerships, examination of funding sources, etc. A key element to these projects would also include risk assessments: whether and to what extent these PRC centers of excellence support PRC defense and public security/surveillance apparatuses. Allied nation governments and research institutions could use this information to inform policies and processes on innovation security and integrity. Having these reports and studies produced by a consortium of international partners also enhances trust and buy-in from our allies around the world.

B. *Sponsor programs, workshops, and training to the international community that focus specifically on building competency and subject matter expertise on China concerning innovation security and integrity*.

Much of the engagements and workshops the State Department has facilitated or sponsored to date have focused on raising awareness of the threats and concerns posed by the PRC's malign influence activities and building institutional processes and procedures for improved governance. These efforts are important, and the State Department has arguably made a significant impact within the international community. However, there are insufficient efforts to build workshops that substantively focus at granular levels on the PRC's policies, programs, tactics and methods, and infrastructures that support malign influence and technology transfer activities. Notwithstanding a training course my organization has developed, I am not aware of any (other) training or workshops on how to conduct due diligence and risk assessments on China that specifically relate to research security and integrity.

C. The Office of Innovation Security and Integrity should create a subdivision that oversees policies, research programs, and international engagements specifically dedicated to research integrity.

There is no US government office or organization that has a dedicated mission of understanding and setting or advising policies on *research integrity*. Research integrity is loosely defined in various policies and is co-mingled conceptually with research security without addressing it specifically. Additionally, transparency and integrity risks are rarely assessed and factored into deliberations over whether to pursue or continue research partnerships with PRC institutions across liberal democracies. There are knowledge and policy gaps that must be addressed. For example, the US government (and the international community) has imposed no costs on the PRC when it corrupts the integrity and trust of our research ecosystems. Upholding our common values requires robust and collaborative efforts from governments and research institutions in liberal democracies, and a new OISI should take a leading role in these issues with support from other federal agencies.

A sampling of mission areas the integrity office within OISI includes:

1) With possible support from other federal agencies (such as NIH and NSF), OISI should work with the international community to fund research programs and build infrastructure for tracking, monitoring, and identifying fraudulent publications.

Current efforts to uncover fraudulent science are largely limited to individuals around the world who monitor scientific publications on a volunteer (unpaid) basis. While academic journal publishers are making some efforts to identify fraudulent activity on their own, as for-profit organizations, there are few incentives (or requirements) for the publishing industry to self-police. OISI and other agencies should sponsor research projects that build tools and methodologies such as the emerging field of "forensic scientometrics" for identifying fake science, citation cartels, authorship-for-sale and other schemes, as well as efforts to force retractions of fraudulent publications. OISI should also lead programs to track and report on frequent offenders: individuals, institutions, and publishers found to produce multiple fraudulent publications.

2) OISI's integrity division should oversee multiple projects and information-sharing mechanisms that track other integrity and reciprocity failures.

OISI should oversee programs and sponsor projects to identify and build formal data-sharing mechanisms and platforms that track a variety of other research integrity issues that heretofore have been largely ignored. Other federal agencies and governments of allied nations should also contribute related information, which would be limited to PRC entities and behaviors of concern to maintain the legal privacy protections of entities in liberal democracies. Examples of areas that should be tracked and shared include:

- Identifying published research where the PRC partners fail to provide underlying data due to PRC data laws. This can help inform decisions on to what extent international partners should collaborate with specific PRC institutions or on specific disciplines if there are high risks of data reciprocity failures.

- Identifying and characterizing instances of transparency failures by PRC research organizations that are intentionally designed to obfuscate their missions, research activities, etc., or mislead or misrepresent such activities.

- Descriptions from governments or research institutions of PRC entities that have acted in bad faith, such as failing to abide by the terms of cooperative agreements; or entities that have provided federal agencies "comfort letters" that are intended to deny and deceive federal regulators or research grant managers.

5. Harden the False Claims Act (FCA) to enforce public institution compliance.

Amend the FCA to include a provision that all public (state) universities or research institutions that apply for and receive federal contracts or grants waive their rights to sovereign immunity claims under the 11th Amendment of the Constitution.

One interpretation of the 11th Amendment[40] is that any state institution, *including public universities*, is immune from False Claims Act civil suits as this equates to the federal government suing a state government, thus violating a state's sovereign immunity. This hampers the ability of federal agencies to pursue false claims cases against state universities. Any public institution should be subject to the same responsibilities, standards of compliance, and fraud provisions as private entities. Waiving state sovereign immunity claims should be a condition for a public university to accept grants or contracts from the federal government.

6. Increase funding for OIG personnel and civil litigation.

Congress should appropriate funding to increase the number of Office of Inspectors General (OIG) agents, attorneys, and support personnel - as well as training to OIG elements - to more aggressively pursue False Claims Act cases. Increases in OIG resources directly result in increases in monetary recoveries by the government that far exceed the additional costs.

FCA litigation has proven to be an effective yet insufficiently pursued civil remedy to punish academic institutions for non-compliance with federal grant and contract rules and conditions. This is especially the case regarding universities' failure to disclose support from the PRC and other foreign sources. Civil false claims cases do not require proof of intent to defraud the government; grant or contract submission documents that contain misrepresentations (or fail to contain required information) are considered false claims.

To be most effective, OIGs and the Department of Justice should more aggressively exercise the law's authority that demands larger penalties (up to triple the amount subject to the false claim) when universities are found liable. This would require the government to demand higher settlement amounts out of court or a willingness to pursue a court's judgment. Enforcing higher penalties as stipulated in the FCA would be a more effective deterrent than the status quo, which to date are simply minor costs of doing business for most universities; most FCA settlements on allegations of false claims amount to a small fraction of the potential liability.

The increased allocation of resources is a budgetary gain, not a deficit because the amount of money that can be recovered through litigation of false claims cases invariably exceeds (sometimes by factors of three or higher) the cost of the increased government personnel and litigation. In essence, it is a substantial return on investment.

7. Federal funding agencies should use grant suspension and debarments more aggressively and modify grant submission certification requirements.

Federal funding agencies should institute policies that more aggressively suspend and debar federal grants to institutions that have lapses in institutional governance and grant

---

[40] The 11th Amendment states: "The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by citizens of another state, or by citizens or subjects of any foreign state."

compliance. Research institutions need to bear greater costs for non-compliance with federal awards. For instance, agencies should suspend all new awards to an institution that has submitted false claims until it can demonstrably show remediation measures have been put in place.

Federal funding agencies should also require that the presidents or CFOs of each institution certify all submissions to the federal government that the information provided in grant or contract documents is complete and accurate.

8. **OIGs and grant program management offices at federal agencies should create a central, government-use only repository of information on the results of investigations, such as findings of non-compliance and false claims**.

The purpose of such an effort is to create a rough equivalent of vendor past performance reports accessible to all grant program managers across federal agencies. Previous judgments or settlements related to fraud or false claims by a university should then be factored into future grant award decisions. Priority should be given to universities that do not have a history of false claims or other non-compliance on competitive awards. Such a repository could also be used for active investigations so that investigators can more easily share information between agencies. Previous investigations have often shown that non-compliance with grants can involve grants from more than one agency.

9. **Pass the DETERRENT Act in the Senate.**

In late 2022, the House passed H.R.5933: Defending Education Transparency and Ending Rogue Regimes Engaging in Nefarious Transactions Act, or the DETERRENT Act. *The Senate should review and pass this bill largely in its current form.* This bill would go a long way in bolstering enforcement of foreign gift, contract, and grant reporting requirements of higher education institutions, especially when supplemented with the other recommendations of this testimony.

10. **Require recipients of NSF CAREER awards to sign a continuing service agreement with the US government.**

The PRC has benefitted from substantial NSF investments in future scientific leaders by recruiting recipients of NSF CAREER awards who relocate to China. To prevent this, NSF should create a new condition that CAREER award recipients must stay in the US and work at a research institution or in the US government for a specific length of time deemed appropriate by NSF and Congress, but should at minimum be equal to the period of performance of the award.

11. **Create new legislation that expands on Sec 238 of the FY25 NDAA by placing restrictions on all federal sources of fundamental research funding if recipient institutions collaborate with select PRC entities.**

Sec. 238 of the FY24 NDAA[41] restricts DoD fundamental research funding to institutions if they collaborate with academic entities listed pursuant to provisions of Section 1286 of the FY19 NDAA. This is a significant and positive step in curtailing research collaborations with PRC military-affiliated research institutions. However, this rule should be applied to all federal funding, and the list of "covered entities" to which funding restrictions apply needs to be expanded to other government-restricted lists.

The current list associated with the requirements of Sec. 1286 is too narrow in scope. Similar to Recommendation 3 on visa restrictions, federal funding on fundamental research should also be denied to institutions collaborating with PRC organizations on the BIS Entity List, the OFAC sanctions list, and DoD's 1260H list of military-affiliated companies (as some of those entities conduct and publish research).

Efforts are also needed to revise and expand on the entities on these various lists. For instance, there are dozens of officially designated "national defense key laboratories" that are excluded from these lists, and many enjoy international research collaboration. There are also "private" and state-owned enterprises that conduct and publish research with international partners that also need to be added, including firms that support PRC public security organs that engage in human rights abuses.

[41] "LIMITATION ON AVAILABILITY OF FUNDS FOR FUNDAMENTAL RESEARCH COLLABORATION WITH CERTAIN ACADEMIC INSTITUTIONS"