Center for Research Security & Integrity

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

Before a Hearing of the U.S. House of Representatives Committee on Science, Space, and Technology – Investigations and Oversight Subcommittee
"Assessing the Threat to U.S. Funded Research"

Subcommittee Chairman McCormick, Ranking Member Sykes, distinguished subcommittee members:

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 persistent challenges in identifying and disrupting China's exploitation of US federally funded research. Over the last 15 years, I have focused on China's research ecosystem and its state-driven technology transfer apparatus. The collection and analysis programs I ran while serving in various capacities in the government provided insights into China's technology and knowhow acquisition strategies and exploitation of US R&D in public and private sectors.

While in government, 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 and vulnerabilities in academia and the US government, including inaction by federal agencies charged with protecting our national and economic security, which was a key source of my frustration and the reason I left federal service in 2021 after 18 years. Two years ago, I started a non-profit organization called the Center for Research Security & Integrity in part to address the impediments to knowledge building and threat mitigation.

In this testimony, I highlight numerous ways in which the PRC exploits federally funded research, academia's systemic non-compliance with federal grant rules and appropriations laws, and the US government's structural impediments and lack of sufficient policy responses to address research security vulnerabilities. I offer illustrative case studies based on my observations while working in the government as well as subsequent research I have conducted post federal service. It is important that we have honest and sometimes uncomfortable conversations about what is taking place so that we can address the issues effectively. Some of the information I provide is rarely discussed publicly, perhaps because it can expose the shortcomings of academia and the government.

The final section lists specific recommendations, some of which involve revising or expanding existing regulations and policies. *However, a key recommendation will require paradigmatic shifts in how the US government approaches research security, particularly in response to China's threats to our research enterprise*.

Table of Contents

Introduction: PRC Methods to Exploit Our Research Ecosystem

The threats and malign influence posed by the PRC on our research and innovation ecosystem and their implications are under-recognized problems. There is insufficient knowledge on how the PRC has and continues to benefit economically and militarily through its mostly unfettered access to federally funded research as well the corrupting and corrosive effects of its influence activities. This testimony seeks to provide insights into the enormity of the problem that the US government has inadequately addressed.

A *sampling* of some of the threats and exploitation by the PRC include:

- Converting or diverting US government-funded research into intellectual property 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 economically.
- Repurposing US research, including in seemingly innocuous fields like climate change 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 US industry and federal and state governments for China's benefit 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 predominantly benefit China.

- Establishing or co-opting networks of organizations in the US that enable knowledge transfer, talent recruitment operations, and PRC state-backed venture capital investments intended to offshore critical technology to China. A subset of this effort includes targeting recipients of US Small Business Innovation Research programs.

- 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 transparency, reciprocity, and other aspects of integrity that equate to deception, fraudulent publications, or other forms of dishonest research and publication practices.

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 the U.S. (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; they have argued that 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 because the U.S. and 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, the US and most of our key allies, have failed to adapt or address 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 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 the willing participation of US academia*. Academic institutions, especially at the individual faculty level, tend to mirror image key aspects of our system with that of the PRC and fail to recognize the incompatible elements – that the PRC's authoritarian system controls and drives most research activities and decisions. While many individual Chinese researchers who work with US academics may share the same values and passion as Americans do in their research endeavors, they are under a system that has specific objectives that run counter to our core values and interests, and those individual PRC researchers have no control over where and what happens to their research. This holds particularly true regarding any data sharing or intellectual property (IP) agreements – it is impossible for any foreign entity to control where data, materials, research, and potential or actual IP goes once it enters China's borders. In fact, the PRC has codified into law its total control and access to all data, information, and materials under the guise of national security, cybersecurity, and anti-espionage statutes.

It is worth noting that based on my observations from supporting federal investigations and conducting due diligence research, most researchers are cooperating with PRC entities (such as defense and surveillance research programs) willingly and voluntarily. The PRC and the CCP has created enormous incentives and opportunities for personal gain by helping the PRC; most of China's efforts to transfer US critical technology do not appear to be coercive in nature.

Federal funding agencies, law enforcement, and intelligence community (IC) elements have done a good job of raising awareness among universities on national and economic security risks associated with some PRC research partnerships. US research institutions conceptually understand 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. 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.*

Previous administrations and academia have argued that any protections or restrictions regarding collaborations with China and other authoritarian regimes should be limited to specified critical technology areas as a so-called "small yard - high fence" approach. Everything outside these designated areas should remain free and open for collaboration. The problem with such an approach is that the PRC has become increasingly adept at diverting many types of STEM research to defense applications, including in fields that may not be included on sensitive or critical technology lists. This is particularly apparent in certain health and climate change fields, such as hearing aid R&D being used to enhance PRC submarine warfare development or climate change research, like remote sensing and marine ecology, enabling next-generation military/surveillance satellites and PLA naval operations.

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

The first restriction (commonly referred to as the "Wolf Amendment") prohibits recipients of NASA research funding from collaborating with most PRC entities on a strictly bilateral basis. I provide further details and case examples of non-compliance with this rule later in this testimony. The second is a restriction stipulated in Sec. 238 of the recently passed FY25 National Defense Authorization Act (NDAA) 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 (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,[1] the government can merely provide guidance on national security risks (if they do at all), but universities can ignore this provided they are compliant with 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 if there are no specific rules that proscribe such activity. However, compliance failures on federal research grants or contracts by US institutions also appear to be widespread and often relate to some form of PRC partnership. The next sections explore these issues in detail.

Research Collaborations of Concern

A key challenge is that responsibility for conducting due diligence and risk assessments currently falls on individual research institutions and faculty overseeing research projects. This is problematic as individuals and institutions do not have nearly enough information or subject matter knowledge on China and its research ecosystem, the current landscape of geostrategic risks and challenges, etc. to make such determinations. It is unreasonable to expect a faculty member who is charged with carrying out scientific research to be able to handle such a task. A lack of information sharing, scholarship, and expertise on the PRC within the US government, including the national security community, is another impediment. If the US government lacks the capabilities and resources, how can an individual faculty member or university handle this on their own?

[1] 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.

National Security Risks

What about partnerships and collaborations with PRC entities that are *widely known to represent national security risks*? The data collated here is a current snapshot of very high-risk US-China scientific and engineering research collaboration. The data is limited to a *sampling* of PRC military entities, weapons R&D facilities, and select defense-affiliated civilian universities. This data **demonstrates US academia's systemic unwillingness to examine national security risks or ethical concerns regarding their research collaborations with China**. Furthermore, the huge scale of these high-risk collaborations suggests dependencies and vulnerabilities that China then exploits.

Tables 1 through 4 break down the number of articles published in 2019 through 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), 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 persistent knowledge gaps on other PRC research institutions that conduct defense research.

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 of these PRC entities 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 innocuous 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 of its citizenry for mass surveillance purposes, and medical research with military applications such as fighter pilot and solder performance enhancements, 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 funders. It is also worth noting that both US government and private sector entities are acknowledged as funders (presumably funding the US researchers). **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 development of 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 and is sanctioned by the US Treasury Department. 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 claim that their research is strictly for commercial purposes (with no dual-use potential), 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, supply other autocratic regimes (especially Russia), and challenge 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.[2] CALT also produces the Dongfeng series of intercontinental ballistic missiles (ICBM)s, the latest versions equipped with multiple independent nuclear warheads able to strike Europe and the Western United States.[3]

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

Some STEM research conducted at these universities is 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' universities and a coauthor affiliated with a US institution.**[4] 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

[2] "China Academy of Launch Vehicle Technology (CALT)," Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59/.
[3] "China Academy of Launch Vehicle Technology – CALT 1st Academy," https://www.globalsecurity.org/wmd/world/china/calt.htm.
[4] 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.

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
Changchun University of Science and Technology	127
Shenyang Ligong University	53

The data in the above tables are admittedly a crude measure.[5] The statistics provide no indication of the nature or frequency of the US collaborations, which are often informal and sometimes unbeknownst to federal sponsors or even the US employers. Investigating these collaborations for approximately 27,000 articles is a daunting task. *Additionally, due to persistent knowledge gaps, this data significantly under-represents the amount 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.

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 restricted dissemination?* This appears to be arbitrary and largely at the discretion of the individual researcher.

The incentive is to avoid addressing 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. The report noted:

[5] 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."[6]

Should all of those articles have been published openly? Should any PRC institution have been allowed to participate in or support 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 key laboratory on radar signal processing at Xidian University (which is co-supervised by China's largest defense electronics and radar systems developer). Thus, research funded by NIH, NSF, and other agencies may affect future US warfighting capabilities.

Ethical Risks: US Research Support to PRC Surveillance and Public Security Apparatus

Academia's indifference to research security concerns is not limited to national and economic security issues. This section demonstrates **academia's persistent indifference to or lack of awareness of ethical risks to 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 engage in human rights abuses. I exclude from this discussion ethical concerns regarding how the research is conducted, particularly as it relates to human subjects.

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,

[6] "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.

including for use in the Xinjiang region used to oppress and detain Muslim minority populations.[7]

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 sample 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 and involve both US and China-based coauthors:

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

Researchers from the US who 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 the party-state will seek 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. Data obtained using the Dimensions aggregator by *Digital Science* included **1,472 articles published 2019 through January 2025 involving US research partnerships with PRC-based entities in these obvious surveillance disciplines.**

Table 6 lists the top 20 US universities ranked by the number of articles published in surveillance-related research with PRC institutions.

[7] 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.

Table 6: Top 20 US Universities Involved in Surveillance Research Collaboration with the PRC

US University	Number of Articles Published 2019 - Jan. 2025
Harvard University	67
Carnegie Mellon University	65
University of California, Los Angeles	59
Johns Hopkins University	54
University of Washington	52
State University of New York at Buffalo	43
Georgia Institute of Technology	41
University of California, Berkeley	41
University of Southern California	40
Stanford University	38
University of Michigan–Ann Arbor	36
University of Illinois Urbana-Champaign	33
Michigan State University	32
University of Pennsylvania	32
University of California, San Diego	32
Temple University	31
Massachusetts Institute of Technology	30
University of Missouri	30
Texas A&M University	29
Cornell University	29

This data represents a small sampling of articles that are easy to recognize as raising ethical concerns. More scholarship is needed to build comprehensive keyword ontologies associated with research disciplines with potential surveillance use and identify PRC research institutions involved. Nevertheless, **this data suggests that US universities have made little to no effort to restrict collaborations with the PRC on ethical grounds and calls into question academia's sincerity in upholding the core values of scientific research they espouse.** Collaborations in these ethically troubling areas can enable or enhance China's continued surveillance and oppression of its citizens *and* the export of related technologies to authoritarian regimes around the world. *If US-based researchers who collaborate with the PRC in this type of research receive federal funding, then this needs to be addressed by relevant agencies and policymakers as part of any effort to bolster research security and compliance efforts.*

I am not aware of any US government efforts or capabilities to monitor formal and informal research partnerships and exchanges between US institutions and PRC entities in areas that have clear surveillance applications. Further complicating any potential compliance or policy objectives are the persistent knowledge gaps on PRC institutions extensively involved in surveillance research and support public security organs. *The US government, particularly the national security community, has failed to systematically identify such entities and share that information with the public.* The Bureau of Industry and Security (BIS) does periodically add some PRC firms to the Entity List for export control purposes if those firms contract with or supply PRC public security organs; but few, if any, efforts have been made to look at PRC academic institutions in this space. Nevertheless, export controls rarely apply to fundamental research, so BIS efforts in this area have little to no impact on research security policies.

US University Non-Compliance on Federal Research Grants and Contracts

In simplistic terms, US universities are 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.

This section discusses universities' known or suspected non-compliance with federal research grant and contract rules and, in some cases, inadequate monitoring and enforcement by federal funding agencies and the national security community in identifying and mitigating the threats to taxpayer-funded research investments. Types of non-compliance are broadly divided into the following areas, though there can be substantial overlap, i.e., university non-compliance with multiple federal regulations simultaneously. These areas relate to:

a) Section 117 of the Higher Education Act
b) Current and pending support disclosures on federal research grant submission documents
c) An appropriations law regarding NASA funding (also known as the "Wolf Amendment")

Section 117 Non-Compliance

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. Additionally, 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. 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. Consequently, *it can be financially advantageous to a US university if they have faculty that holds concurrent appointments in China, regardless of*

whether such appointments or commitments comply with federal grant and contracting rules.

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.[8] 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.[9] A report issued in late 2020 by the Department of Education revealed more than $6.5 billion in previously undisclosed foreign 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."[10] Federal agency enforcement of this law has been minimal, partly due to a lack of willingness by the Biden administration to devote resources to investigate and prosecute non-compliance. Passage of the DETERRENT Act by Congress would go a long way in bolstering reporting requirements by universities and punitive measures for non-compliance.

Given the widespread non-compliance of Section 117 reporting requirements, a few investigators at Offices of Inspectors General (OIG) have initiated proactive investigations with the Department of Justice to determine whether university non-disclosure of foreign gifts or grants (especially from China) was also not disclosed on federal research grants. Civil litigation against universities has demonstrated this to be the case. However, as discussed in the **Recommendations** section of my testimony, to date, such efforts by federal investigators have been quite limited in scope due to a lack of subject matter expertise, experience, and resources.

Current and Pending Support Disclosure Failures

Federal agencies that award research grants require applicants to disclose current and pending support, the details of which have been clarified and expanded on through National Security Presidential Memorandum-33. Nevertheless, based on my experience working with federal investigators, *non-disclosures by university grant applicants persist and appear to be widespread.* The types of current and pending support that are required to be disclosed on grant submissions include any material support to a research endeavor, such as personnel or equipment and sources of funding (contracts, grants, etc.) that relate to the proposed research (or during the conduct of the research if already underway).

Some universities have not disclosed contracts, gifts, or research grants they received from China as current and pending support on federal grant applications and periodic report

---

[8] See 20 U.S. Code § 1011f.
[9] "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.
[10] "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.

submissions. The disclosure failures can be attributed to individual principal investigators (PIs), university administrators, or both. Technically speaking, universities are the recipients of federal grant monies, which are then disbursed to the PIs; thus the universities are the responsible parties that certify the accuracy of information on grant submission documents. This also means that it is more effective for federal agencies to hold universities accountable through civil remedies (e.g., using the False Claims Act) than attempting to indict or convict an individual faculty member (PI) on criminal charges for providing false statements to the federal government.

That said, it is important to understand that PRC state-sponsored talent programs often contractually obligate and instruct selectees (in this case, US PIs and co-PIs on federal grants) not to disclose details on their level of commitment, sources of funding, projects, or positions in China to their US employers. This means that the US universities that employ them may not always be aware of these commitments, which leads to federal grant non-compliance as the PIs are also failing to disclose their current and pending support on grant applications. Universities have recognized this as a problem, and many have revised or bolstered internal activity reporting and related policies and procedures so that administrators can be more fully aware of the engagements and commitments of their faculty.

However, this is not the whole story. *Federal investigations discovered that some universities have been complicit in grant disclosure failures*. Their motivations are probably monetary in nature. 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. To be fair, it is important to note that US academia is not monolithic; I am not suggesting every institution operates in the same unscrupulous ways described in this testimony. Some universities, for example, have robust research security and compliance programs that seek to serve as responsible stewards of taxpayer money and cooperate closely with federal agencies to ensure continued compliance.

Two recent civil cases described below are illustrative of these disclosure failures and their implications.

Example 1: Stanford University Settlement Agreement

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).[11] The US alleges that these disclosure failures violate the False Claims Act. The case was resolved through a settlement

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

agreement between Stanford University and the US government, whereby Stanford agreed to pay $1.9 million to resolve allegations of False Claims Act violations.

Interagency efforts to pursue civil remedies should be lauded as they are a much more effective and fairer approach to mitigating these concerns compared to pursuing criminal prosecutions. 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, this small settlement agreement is unlikely to create any real deterrent for universities to change their behavior. The penalties to date largely equate to a modest cost of doing business; 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.

Example 2: University of Maryland Settlement Agreement

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[12] 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."[13] Note that the first project clearly has mass surveillance applications. UMD agreed to pay $500,000 in the settlement agreement. Like the Stanford case, this represents a small percentage of penalties UMD may have been liable for if a court ruling was pursued.

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 have claimed 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 they do 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.

---

[12] PI refers to principal investigator, the researcher(s) that leads a project funded by federal research grants.
[13] https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed

A secondary and largely unaddressed compliance concern may also be taking place. Unrestricted gifts may not 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 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 could be considered fraud.

There are other secondary and corrosive effects that are not being adequately discussed in public discourse. When universities or their faculty fail to disclose these outside sources of funding (regardless of whether they are 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. Furthermore, federal research grants are highly competitive; only a fraction of the total grant 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? 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.

'Wolf Amendment' Non-Compliance

An appropriations law in effect since 2012 places "Chinese Funding Restrictions" on any NASA-funded grants or contracts. The law, which is also referred to as the "Wolf Amendment," statutorily prohibits recipients of funding from NASA from engaging in bilateral participation, collaboration, or coordination with the People's Republic of China, Chinese-owned companies, or Chinese universities.[14] Multilateral research exchanges involving China and any additional country are exempt from this restriction. NASA has provided clear guidance to universities on this rule since it has gone into effect. Nevertheless, an unknown number of US institutions receiving NASA funding have violated this law through bilateral research collaborations with PRC institutions. A cursory analysis of research collaborations a colleague and I have conducted suggests that university non-compliance is widespread.

Universities receiving NASA research funding must comply with this appropriations law and by receiving such funding, they certify compliance. Universities that violate the Chinese

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

funding restrictions are submitting false claims to the federal government (i.e., fraud). An example of a Wolf Amendment violation is a recent case against the University of Delaware.

Case Example: University of Delaware

On December 10, 2024, the Department of Justice (DoJ) announced that the University of Delaware (UD) would pay a $715,580 fine for failing to disclose a prominent UD researcher's "affiliation with and support from" the PRC government.[15] The UD professor, Dr. Xiao-Hai Yan, was a PI on a NASA grant identified in the settlement agreement who concurrently served as a prominent research faculty member at China's Xiamen University. Professor Yan received substantial research funding from the PRC government and was a "Thousand Talents Program" selectee.

A colleague and research partner LJ Eads[16] and I conducted our own research on Professor Yan and his activities in China. Dr. Yan is a recognized expert in oceanography and remote sensing research; his contributions to deep ocean remote sensing and climate change research have been recognized by both the US and PRC governments. Yan served as Director of UD's Center for Remote Sensing and Associate Director for the NASA-Delaware Space Grant Consortium beginning in 2005[17] (to which NASA obligated nearly $10 million in federal grants and a cooperative agreement with UD).

Dr. Yan was a PI or co-PI on numerous NASA grants (as well as Navy and National Oceanic and Atmospheric Administration grants). At the same time, Yan held appointments in China, including positions at Xiamen University from at least 2007 to the present, thus engaging in ongoing and substantial, bilateral collaborations with PRC entities (a violation of the Wolf Amendment since 2012). Professor Yan also played a key role in establishing several cooperative agreements and joint training programs between UD and Xiamen University, including a joint remote sensing research center and the construction of a satellite ground station at Xiamen University. Some of these formal agreements were established *after* the Wolf Amendment became law. It is not known whether UD received any funding from the PRC, such as a gift or contract, as part of these cooperative agreements. Nevertheless, at least some of these activities almost certainly involved NASA funding sources. In other words, both Professor Yan and UD leadership demonstrated willful negligence or disregard for US appropriations law.

Even more troubling is the fact that Professor Yan led a research and engineering project at Xiamen University to develop a new synthetic aperture radar (SAR) satellite in partnership with several PRC defense state-owned enterprises. One of these PRC firms, Spacety China, is now sanctioned by the Treasury Department for its role in providing satellite imagery to Russia for targeting Ukrainian infrastructure.[18] Yan's activities in China and his involvement in US federally funded research that threatens US national security are extensive and far exceed the scope of this testimony.

---

[15] https://www.justice.gov/usao-de/media/1380506/dl?inline
[16] LJ Eads is a former US Air Force intelligence analyst and now the founder of Data Abyss, an S&T intelligence platform of Parallax Advanced Research.
[17] https://www.udel.edu/content/dam/udelImages/ceoe/documents/smsp/Yan_Xiao-Hai_2page.pdf
[18] https://sanctionssearch.ofac.treas.gov/Details.aspx?id=40477

The Chinese funding restrictions stipulated in the Wolf Amendment are intended to prevent the transfer of technology and knowhow from NASA-funded programs to China. The DoJ and NASA were right to investigate UD for its false certifications that NASA funding was not being used in scientific collaborations with China and hold UD accountable for its non-compliance. However, the UD settlement appears quite low compared to UD's potential liability and may not serve as much of a deterrent for non-compliance. The settlement agreement is the only publicly known action the government has taken to date. If it has not already, the US government should also address these questions:

- There were several grants whose period of performance were after the 2012 appropriations law went into effect, during which time Yan held concurrent positions in the PRC. Why did prosecutors limit litigation to just one of the many NASA grants Yan served as PI or Co-PI on? Why did it take 12 years for investigators to identify non-compliance?
- Were the UD centers that receive NASA funding also a potential Wolf Amendment violation? What about the other UD-Xiamen University cooperative agreements?
- Professor Yan's concurrent positions in China have taken place for over 20 years, some of which have involved partnerships with very high-risk defense entities. Why didn't the US national security community attempt to mitigate or disrupt this activity?

In my opinion, most of the government's shortcomings relate to a lack of investigative resources or priorities (or both) to aggressively pursue compliance monitoring and enforcement and a lack of subject matter knowledge on how to identify these threats and mitigate them when they do not involve illicit activities.

Case Example: University of Maryland's Apparent Violations of the 'Wolf Amendment'

Through our own research, LJ Eads and I have identified another case where violations of Chinese funding restrictions of the Wolf Amendment are probably taking place. A summary of findings of apparent non-compliance follows, which were based exclusively on self-funded efforts: we have received no materials, information, funding, or any other form of support from any federal agency that relates to this matter. This information is derived from surveying the University of Maryland's (UMD) receipt of NASA research grants and cooperative agreements, as well as concurrent bilateral research collaborations with PRC researchers and institutions that likely violate Wolf Amendment restrictions.

Due to its proximity to NASA's Goddard Space Flight Center in Greenbelt, Maryland, UMD has cultivated a close research partnership with NASA. Since 2010, a memorandum of understanding has underpinned joint activities in space-based science, engineering, biosciences, earth sciences, and education. This longstanding relationship has enabled UMD to be one of NASA's top sources for future scientific and engineering talent.[19]

Through analysis of public information on grant and contract award data,[20] we determined that Since 2013, UMD has been the recipient of at least 36 NASA research grants and contracts. We also examined the Earth System Science Interdisciplinary Center (ESSIC) at UMD, which operates under a $95 million cooperative agreement with NASA. To date, NASA

[19] https://research.umd.edu/partnerships/government/partnership-overview-nasa
[20] Federal award data was retrieved from usaspending.gov.

has obligated approximately $85.4 million under these awards in aggregate. However, public reporting discrepancies and potential unrecorded awards likely underestimate actual NASA award amounts.

Surveys of scientific publications and supplemental research suggest widespread non-compliance with the Wolf Amendment by dozens of UMD faculty and staff researchers at ESSIC. This includes over 40 research publications coauthored by at least 30 UMD personnel - professors who are PIs / co-PIs on NASA grants or ESSIC staff researchers – that have engaged in what appears to be strictly bilateral collaborations with PRC institutions. Additionally, a few UMD faculty members involved in NASA-funded research appear to hold or have held concurrent positions at PRC universities, which may also be a violation. To assess non-compliance, further investigation is required to determine the exact nature of these collaborations and the research involved (i.e., to determine if the underlying research was based on NASA funding).

Some of the observed research papers credit both NASA and PRC government funding sources as supporting the research, including PRC defense funding. This raises national security concerns as it may facilitate the transfer of sensitive technology and data to the PRC institutions.

A few examples of strictly bilateral US-China research collaborations that have dual-use applications include:

- UMD Associate Professor Dongdong Wang led a study published in January 2018, titled *"Evaluating Land Surface Albedo Estimation from Landsat MSS, TM, ETM+, and OLI Data Based on the Unified Direct Estimation Approach."* This project is particularly concerning because the PRC funding sources clearly show China's strategic interest and defense application potential. PRC funders included the National 863 Program, the National Natural Science Foundation of China, the National Key Research and Development Program of China, and a National Defense Project of China.[21] China's 863 Program (now consolidated into a newer funding line) was focused on applied research and heavily involved in defense programs.

- UMD Professor Ning Zeng coauthored a December 2020 article titled *"Spaceborne Detection of XCO_2 Enhancement Induced by Australian Mega-Bushfires."* This study involved PRC co-researchers from Nanjing University and the Chinese Academy of Sciences. Some of the acknowledged funding includes multiple NASA grants as well as the National Natural Science Foundation of China and the National Key R&D Program of China.[22] The research involved sophisticated remote sensing techniques that could be repurposed for military applications.

- In June 2021, UMD Professor Sylvain Veilleux coauthored a study titled *"A Broadband Si_3N_4 Polarization Beam Splitter Based on Asymmetric Directional Couplers."* The study included a Chinese co-researcher from the Key Laboratory of Quantum Information at the University of Science and Technology of China.[23] Although primarily funded by NASA, the involvement of a

[21] https://doi.org/10.1016/j.rse.2017.10.031
[22] https://iopscience.iop.org/article/10.1088/1748-9326/abc846
[23] https://ieeexplore.ieee.org/document/9597974

leading PRC quantum information laboratory in developing advanced photonic technologies at a PRC university known to be extensively involved in defense research raises serious national security concerns. Such dual-use technologies are critical in the realms of secure communications and defense applications.

Additionally, several UMD researchers have maintained dual appointments or affiliations with PRC institutions. These positions are not merely honorary; they often entail active participation in research projects, curriculum development, and strategic collaborations with their Chinese counterparts. Such arrangements can facilitate the regular exchange of ideas, methodologies, and, in some cases, sensitive research findings. Notable examples include, but are not limited to:

- UMD Associate Professor Dongdong Wang has held a concurrent position at Peking University's Institute of Remote Sensing and GIS at the School of Earth and Space Sciences, *while serving as a NASA PI on several grants*.[24] The Institute of Remote Sensing and GIS faculty webpage of lists Wang as an Associate Professor and Changjiang Chair Professor.[25] The latter refers to the Changjiang Scholars Award Program, one of China's most prestigious talent recruitment programs that seeks experts from overseas to transfer technology and knowhow to China.
- Professor Zhanqing Li from UMD's ESSIC held a concurrent affiliation with the State Key Laboratory of Earth Surface Processes and Resource Ecology at Beijing Normal University.[26] *While Professor Zhanqing Li was a NASA PI*, he was also a PI for China's "973 Program" on a project titled "Observation and Modeling of Climate Effects by Clouds and Aerosol." That project appeared to run from January 2013 to August 2017 at the State Key Laboratory of Earth Surface Processes and Resource Ecology.[27]
- (Now Emeritus) Professor Shunlin Liang held a dual appointment at UMD and Wuhan University[28] and led significant remote sensing projects in China while working on NASA-funded research.

We identified numerous other examples of bilateral collaborations that may violate Wolf Amendment restrictions, such as multiple UMD researchers who visited China to provide lectures and participated in exchanges at PRC institutions (e.g., visits to Beijing Normal University, Peking University, and the Chinese Academy of Sciences) while concurrently serving as NASA PIs. *The examples discussed here merely scratch the surface of identified bilateral research collaborations and exchanges involving NASA-funded researchers. The scope of this activity suggests a systemic, institution-level disregard for compliance with NASA grant and contract rules.*

In addition to the government's lack of sufficient personnel and subject matter knowledge to pursue investigations of federal grant non-compliance, there may be another reason why OIG offices and DoJ have not aggressively pursued False Claims Act (FCA) cases against

---

[24] https://www.sciencedirect.com/science/article/abs/pii/S0048969724069407?via%3Dihub
[25] https://irsgis.pku.edu.cn/ls/ygcs/wdd/index.htm
[26] https://acp.copernicus.org/articles/18/8995/2018/
[27] https://espre.bnu.edu.cn/english/research/presentprojects
[28] http://www.lreis.ac.cn/kfjl/sjlt/201807/t20180716_416275.html

UMD and other public universities: fear that public universities may assert 11th amendment-based sovereign immunity protections against their misdeeds.[29] This area of the law appears to be unsettled and largely untested. Therefore, perhaps understandably, risk-averse prosecutors may sometimes prefer not having to face that challenge, *potentially slowing the successful pursuit of civil claims against noncompliant public universities.*

It is encouraging that DOJ's recent FCA civil actions against the universities of Delaware and Maryland discussed earlier in this testimony indicate that both DOJ and the public universities it pursued the claims against did not believe assertions of sovereign immunity by public universities in these sorts of cases would be successful. However, it is also possible that the universities of Delaware and Maryland simply decided it was in their best interests to cut their losses and tie up those matters as quickly as possible, particularly given that the scope of their FCA violations could have been far greater than the (small) amounts of the settlement agreements.

Other PRC Threats, Influence Over Federally Funded Research

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 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. Primers on the PRC's talent programs have been published elsewhere and thus are not included in this testimony. This testimony sheds light on lesser-known or understood elements of these programs that have affected federal funding of scientific research.

Some academics argue that the US government has exaggerated the risks and threats posed by China's state-sponsored talent programs. 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 PRC's government-led human capital investments do share similarities with those of the US and other nations: to help advance science and technology to bolster a country's economic development.

However, this 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

[29] The 11th Amendment of the Constitution 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."

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.

Many elements of PRC talent programs encourage insidious behaviors. Selectees of these programs can have corrupting effects on our academic institutions, exploit individual and institutional vulnerabilities through money and resources, undermine core values of academic research such as integrity and transparency, engender conflicts of interest 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. The following case examples illustrate some of these insidious behaviors that threaten the security *and integrity* of our research enterprise.

Example A: Corrupting NOAA Research and Operations

An investigation I supported when I was in the government illustrates ways in which talent programs can involve malign influence and create corrosive effects on our research. This case is also important because it shows federal research facilities (such as our national laboratories) are also affected, not just universities. In this case, the 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 with a foreign government.

However, the requirements of the PRC talent program appointments were the most concerning with respect to malign influence, many of which are not illicit acts. 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 and repeatedly 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 that listed him as exclusively affiliated with a PRC institution during his tenure at NOAA.

- Facilitate academic exchanges and formal partnership agreements between NOAA and the PRC institutions the subject held concurrent positions at, 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 merit-based hiring practices. At a minimum, this undermines the integrity of our open system; more damaging is when individuals are carrying out research projects conducted by specific individuals at the behest of the PRC party-state in critical technology fields and creating/controlling a talent pipeline strictly for China's benefit.

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; 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.

Example B: 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 representing 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 (based in China and the US). In other words, he was commercializing federally funded research for personal (and arguably China's) benefit.

Professor 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 counterintelligence 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 remained in government. Zhu recently relocated to China and now leads a massive AI research effort there, as reported by *Newsweek.*[30] 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. Thus, the US taxpayer -- especially through DoD – funded and trained multiple generations of PRC scientists in critical technology fields that are now at institutions supporting PRC military and public security organs.

It is highly probable that Zhu's appointments in China and activities with his companies may have violated federal grant rules, especially regarding disclosures of current and pending support and affiliations in China. Even if Zhu's actions were not illicit in nature and thus a criminal investigation was not warranted, the US government could have pursued civil remedies, such as through OIG investigations, and would have likely found systemic non-compliance with federal grants. Through civil and administrative remedies, federal agencies could have denied funding to Zhu and his programs at UCLA, which in turn could have prevented him from building a hiring pipeline of PRC nationals for his (and China's) benefit;

---

[30] 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.

and his lack of access to DoD funding would also make him less desirable to PRC institutions that recruited him. If US government national security elements had worked with OIG components and acted swiftly, much of the knowledge transfers to China, funded largely by DoD, may have been prevented. We must learn from these unforced errors.

Example C: 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 are not federal employees but are subject to provisions of law governing the ethics and conduct of federal employees.[31]

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 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 become 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 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 nearly 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 PRC malign influence over federally funded research.[32] *Based on my experience, it appears that the scale and scope of PRC influence activities over federal grant award decisions are largely unknown.*

Example D: 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

---

[31] https://new.nsf.gov/careers/rotator-programs/intergovernmental-personnel-act-ipa-assignments

[32] 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 here again, it is not known to what extent this has taken place.

are nearing completion of their term as an NSF CAREER awardee. "The Faculty Early Career Development (CAREER) Program is an NSF-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 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."[33]

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.

Example E: Exploiting SBIR Programs

PRC talent programs and state-backed investment entities 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 PRC state-funded 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).

US-Based Support Networks for PRC Technology Transfer Activities

There are organizations in the US that demonstrably partner with, take tasking and direction from, or serve as a proxy to Chinese Communist Party (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 often support 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

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

and dissemination of that information is considered government use only.[34] However, I can offer some key findings:

- 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. Leadership of these organizations run 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.

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.[35]

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. **When both the US government and academia espouse "common values" of transparency, integrity, and reciprocity but impose no cost to PRC 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 measures to mitigate PRC practices that undermine research integrity, even when federal research funding is affected.*

My non-profit's latest publication catalogs numerous ways China has violated these norms and the implications of academia and government inaction.[36] 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

---

[34] 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)

[35] "G7 Best Practices for Secure & Open Research," Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, May 2023.

[36] 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.

by far the world's largest producer of fraudulent publications, which has a profound impact on trust in the global research enterprise.

The issues described in this study should warrant rigorous policy responses from both the government and academia, yet their 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. A *sampling* 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 interests or outside involvement (as a shareholder, company board member, founder or chief scientist/engineer of commercial firms) on any CV, faculty page, grant, or (co)authored publication

PRC entities that lack transparency or integrity undermine trust, complicate the US government and academia's due diligence and risk assessment efforts, and create an unsecured research environment. Additionally, 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 can 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.[37]

This "comfort letter" provided to the US institution was intended to deny and deceive NIH, and it being 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.*

Reciprocity

Issues of reciprocity are also not receiving scrutiny, and the US 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 cooperation 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, however, 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.

Another issue is that 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 specific 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.*

US Government Challenges and Impediments to Building Robust Research Security Programs and Policies

Up to this point, I have described the numerous ways in which the PRC exploits federally funded research, academia's systemic non-compliance with federal grant rules and

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

appropriations laws, and a lack of policy responses by both academia and the government in addressing research security vulnerabilities. This section focuses on the US government's structural impediments, failures, and knowledge and policy blind spots that impede its ability to monitor and enforce compliance on federal research grants and contracts and to protect our early-stage research and innovation ecosystem more broadly. (The final section of this testimony offers recommendations that the legislative and executive branches can implement that specifically address these deficiencies.)

Most of the structural impediments and failures by the US government to adequately protect federal research investments discussed below are based on my observations supporting national security, law enforcement, policy, and OIG elements, as well as engagements with executive leadership of federal agencies. I will break down the challenges by first examining strategic and structural issues, followed by more tactical areas. It is worth noting that a few individuals in the US government (in addition to myself) have pointed out these challenges and have recommended to executive branch leadership some of the solutions described in this testimony since early 2021 or, in some cases, even earlier. To date, however, these problems have persisted and remain laregly unaddressed.

Policy Gaps

As noted in this testimony, there are only two rules currently in effect that restrict research collaborations or partnerships with PRC entities within fundamental research domains: a) the Wolf Amendment that bars recipients of NASA research funding from engaging in any bilateral collaborations with China unless a Congressional waiver is applied; and b) a newly instituted provision (Sec. 238) of the FY25 NDAA that will restrict recipients of DoD funding in fundamental research areas if they collaborate with a select group of PRC entities. However, the current list of entities that apply to this policy is inadequate and needs to be expanded.

Recipients of fundamental research grants or contracts from any other federal source face *no other restrictions or limitations on national security grounds*. Academia is free to work with any PRC organization of their choosing, even if those same entities face trade restrictions (export controls) or sanctions. The over 27,000 articles involving US researchers and the PLA, PRC weapons R&D and production facilities, and other defense research organizations attest to the fact that academia does not take research security seriously when there are no specific prohibitions in place.

Similarly, there is no clear policy proscribing research funding if recipients partner with authoritarian regimes on research with potential applications in mass surveillance and human rights abuses. Program managers overseeing federal research grants and contracts do not appear to take this into account when awarding research dollars to institutions. Universities are either unaware that ethically troubling research collaborations are taking place or turn a blind eye to them.

The government also lacks policies to address integrity, transparency, and reciprocity issues, even when federal research funding is affected. For instance, federal agencies like NIH do not share information on the "comfort letters" it has received from PRC institutions that

provide false statements to obstruct grant compliance investigations. The PRC entities engaging in dishonest practices do not appear to face any repercussions for their actions, i.e., agencies have set no restrictions or conditions on funding to entities that partner or collaborate with these dishonest PRC organizations. The same goes for situations where a partnering PRC institution fails to share data or materials that went into published findings, including research (co-)funded by the US government. Neither the government nor academia appears willing to impose any costs on PRC institutions when they violate the core principles and values of academic research.

Intelligence Community and Law Enforcement Shortcomings

Structural impediments persist within the intelligence community (IC) and law enforcement components such as the FBI and military department investigative units. China's state-supported technology transfer apparatus targeting unprotected and unregulated areas dwarfs illegal or espionage activities, yet the latter have monopolized US government attention and resources. Messaging by the US government that China is stealing secrets from academia is misleading and misguided. The following are examples of the shortcomings that leave federal research investments vulnerable to exploitation by China.

- Law enforcement elements focus largely on identifying criminal activity; in cases of technology transfer, this means critical knowhow or intellectual property has already been transferred or stolen, i.e., cases usually involve showing the damage that has been inflicted, rather than protection and disruption efforts.

- The counterintelligence community has not sufficiently adapted to post-Cold War realities, especially with China. A myopic focus on chasing PRC spies leaves most of our research unprotected, given China's tactics within fundamental research domains 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.

- The IC's over-reliance and imputed value on classified information sources limits the government's ability to share information with public and private sectors. This situation has been worsened by a multi-decade erosion, descoping, and devaluation of open-source intelligence within the IC and has led to unaddressed and yawning knowledge gaps.

Lack of Expertise

A dearth of Mandarin language-capable analysts and subject matter experts in the IC and law enforcement has led to a fundamental lack of understanding of the magnitude and complexity of China's state-supported technology acquisition and transfer apparatus. This has created additional challenges, including:

- 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 receiving advanced degrees 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.

- Ineffective messaging to the public by the national security community. Most officials conducting public outreach do not have relevant experience or knowledge, which limits their ability to address specific questions from audiences or have information available that is tailored to those entities. The standard model of providing general talking points for law enforcement agency field offices’ use is not effective at building trust and confidence with the private sector and academia.

- Analytic components in the IC are not mandated to perform or are evaluated on due diligence or vetting requests. The lack of any significant support to US research institutions regarding research security and integrity has placed the burden of conducting due diligence and risk assessments almost entirely on individual institutions.

- Persistent knowledge gaps on PRC academic and commercial entities conducting R&D tied to defense and public security apparatuses limit the government’s ability to identify risks, especially in critical and emerging technology fields.

Grant and Contract Compliance Monitoring and Enforcement Shortcomings

The aforementioned challenges also negatively affect the US government’s ability to monitor and enforce compliance with federal research grants and contracts. Much of the shortcomings listed below stem from a lack of common standards for assessing risk, minimal capacity to conduct due diligence, an unwillingness to share data among agencies, and a critical shortage of experienced investigators who have the requisite subject matter expertise to pursue civil, administrative, and criminal investigations relating to federal grant compliance.

Deficiencies with Vetting, Due Diligence, and Compliance Investigations

Each agency has its own research security and due diligence process; there are no consistent methodologies or standards for assessing risks across federal agencies. Within the DoD, different program offices conduct varying levels of due diligence (if any) and have their own standards or rules that may be inconsistent and uncoordinated across the defense enterprise. There is also no central place where offices can check for existing derogatory information on grant or contract applicants to do simple due diligence checks.

Proposers on grants or SBIR contracts have been observed to “shop around” – if one agency or component denies an award based on assessed national security risks (e.g., foreign ownership, control, or influence), they will apply to another element and sometimes get awarded due to no common standards for risk. When I worked in the DoD, on more than one occasion, due diligence checks by one intelligence component found derogatory information showing ties to hostile foreign entities that pose a national security risk. Several DoD components chose to decline to award a contract, but one component ignored the derogatory information and allocated funding anyway.

Other deficiencies include, but are not limited to:

- Many program offices that award research grants or contracts to academia lack comprehensive tools, technical solutions, or capabilities to assess risk or screen grant applicants for potential national security concerns. In one observed case, an academic applied for a research grant on a project that was already funded by the PRC, but this was not discovered until after the grant was awarded due to a lack of capabilities and subject matter knowledge of the program offices. Additionally, some DoD program offices lack sufficient information on grant applications and documentation on all individuals supporting the research other than principal investigators (PIs).

- Vetting of foreign nationals prior to grant or contract award, if done at all, is insufficient: the PRC party-state targets, recruits, and co-opts individuals *after* they have expertise and access to critical research in the U.S. (many of whom are US citizens). The US government has few resources or processes in place to monitor for national security risks *post award* of a grant or contract.

- A lack of data sharing between agencies results in duplicative due diligence and risk assessment reviews. This also handicaps fraud or other grant compliance investigations when more than one agency is affected, which is not uncommon. When I was in the government, I supported a Foreign Influence Investigations Working Group (FIIWG) made up of OIGs, DOJ prosecutors, and military investigative elements. The working group's intent was to share data and information and assist investigations across agencies. However, information sharing was voluntary, and different agencies had varying priorities and data-sharing rules that led to a general unwillingness to share information.

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

- A dearth of analytic and subject-matter expertise to conduct due diligence and knowledge on how to investigate criminal, civil, administrative, and compliance issues related to research security. I am aware of only a few individuals who remain in the government who have a high level of understanding and experience of how to conduct the analysis and investigations related to university non-compliance with federal grants and contracts.

Recommendations for Policymakers

The challenges we face in protecting federally funded research are daunting due to extensive exploitation and malign influence by China, systemic non-compliance by universities on federal awards, a lack of sufficient research security measures or policies by either academia or the US government, and structural deficiencies within the national security and law enforcement communities.

On February 21, 2024, the White House issued a new presidential memorandum titled "America First Investment Policy." This document calls for developing new measures to "reduce the exploitation of public and private sector capital, technology, and technical knowledge by foreign adversaries such as the PRC." The policy also includes creating or expanding restrictions on US outbound investment in the PRC relating to critical

technologies, such as semiconductors, artificial intelligence, quantum, biotechnology, hypersonics, aerospace, advanced manufacturing, and directed energy areas that all have dual-use/defense applications.[38]

Interagency efforts to prevent PRC's acquisition and further development of these areas outlined in this new investment policy will not be effective if there are no corresponding policies and protection measures put in place within our research ecosystem, as this is where the talent and technology development originate. To address the problems described in this testimony, we must aggressively break down silos and build new paradigms within the government. *Simply appropriating additional resources for existing research security efforts, for example, will achieve little if the structural and knowledge deficiencies are not addressed.*

This final section offers recommendations that seek to: a) address persistent knowledge, regulatory, and policy gaps; b) re-align academia's incentives that better comport with US national interests; c) create efficiencies and cost savings to the US government in compliance monitoring and enforcement; and d) limit the PRC's near unfettered access to federally funded research and impose real costs to China when it violates commonly accepted norms and values.

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. Reducing federal investments in R&D will complicate any protection and research security measures we put in place, as this will incentivize academia to further pursue partnerships with and/or accept money and resources from China to make up the shortfalls.

1. Pass the DETERRENT Act.

The Defending Education Transparency and Ending Rogue Regimes Engaging in Nefarious Transactions Act (H.R. 1048), also known as the DETERRENT Act, has been re-introduced in the House as the last Congress failed to pass the bill. This Congress *should review and pass this bill largely in its current form.* The 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.

2. 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 that relocate to China. To prevent this, NSF

[38] https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/

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 as determined by NSF and Congress, but should at minimum be equal to the period of performance of the award.

3. Create new legislation that places restrictions on all federal sources of fundamental research funding if recipient institutions collaborate with select PRC entities.

Sec. 238 of the FY24 NDAA[39] 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. *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. 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 the entities on these various lists. This should be a line of effort discussed in more detail in **Recommendation 6.**

4. Federal funding agencies should more aggressively use grant suspension and debarments.

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

5. Revise appropriations law or require federal agencies to insert new requirements on all federal research grants and contracts that state that all recipients of federal funding will be subject to the False Claims Act.

One legal interpretation of the 11th Amendment 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, which would violate a state's sovereign immunity. This hampers the ability of federal agencies to pursue False Claims Act cases against state universities. *Any public institution should be subject to the same responsibilities, standards of compliance, and fraud provisions as private entities. Waiving any 11th Amendment*

---

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

immunity claims should be a condition for a public university to accept grants or contracts from the federal government.

6. Authorize NSF to Create a National Research Security, Integrity, and Compliance Center and enable a corresponding interagency investigative task force.

The NSF Office of the Chief of Research Security, Strategy & Policy and NSF's OIG have arguably been the most effective and forward-leaning within the US government in building an infrastructure for leading and enhancing research security policies, programs, grant compliance investigations, and information sharing efforts across the US government. Some of these efforts are still in their early stages, but the infrastructures and knowledge already in place allow for greatly expanded efforts to address the government's impediments and deficiencies described in the previous section. **Policymakers should support the establishment of a new structure at NSF, notionally referred to here as the National Research Security, Integrity, and Compliance Center (NRSICC), that greatly builds upon existing efforts AND consolidates all US government-wide approaches to research security and integrity policy development, vetting, due diligence, risk assessments, and grant and contract compliance monitoring and enforcement.**

Consolidating all efforts into one central entity should lead to very substantial cost savings and greatly improve the US government's efficiencies and effectiveness in securing our research ecosystem from China's (and other adversarial nations) predations, as well as address the systemic non-compliance by US research institutions. **The recommended functions of the new center would be self-sustaining in terms of costs to operate; i.e. no additional appropriation of funds would likely be needed.** A detailed concept of operations exceeds the scope of this testimony; the following summarizes key lines of effort, structure, goals, and cost savings.

NRSICC Lines of Effort

A. Consolidated Data Analysis, Due Diligence, Risk Assessments, and Support to Government Investigations

All applications, periodic submission reports, and related documents pertaining to all fundamental research grants, cooperative agreements, and SBIR/STTR contracts awarded by all federal agencies should be housed at the Center. All government offices conducting fundamental research and SBIR/STTR due diligence will be detailed to the Center. This will streamline and ensure fundamental research due diligence is done by a single entity with a single set of risk assessment standards and mitigation framework.

- NRSICC will create and manage a single list of foreign entities and programs that are sanctioned, violate export control laws, or represent national and economic security risks. This includes but is not limited to: foreign malign talent programs, foreign defense research and industrial base entities, entities involved in committing human rights abuses, and any other entity or program that engages in the transfer or diversion of human/intellectual capital, technology, knowhow, or other ethically troubling activities.

- NRSICC analysts will conduct deep-dive due diligence research and analysis on all government (fundamental) research grants and SBIR/STTR contracts to determine risk levels and/or prohibitions/denials of funding. Analysts will also perform data analysis and research to generate leads for law enforcement when suspected criminal, civil, or administrative violations are identified.

While not directly part of the proposed Center, a law enforcement task force made up of OIG agents, auditors, and support personnel, DoJ prosecutors, and other law enforcement components across the government, will formally work with the Center. *This task force will be assigned to exclusively pursue civil (such as False Claims Act) and criminal compliance investigations based on the data and analytic support provided by NRSICC*. NSF's Office of the Chief of Research Security, Strategy & Policy has already built an internal tool for identifying potential non-compliance by NSF PIs or co-PIs. This capability would be incorporated into the functions of NRSICC and be expanded to ingest and analyze all other federal agency data.

B. Due Diligence, Risk Assessment Support to Academia, Private Sector

NRSICC data analysis, due diligence and risk assessment efforts would not just be limited to government award decisions and compliance investigations. The Center would also provide direct support to public and private institutions that have received or are applying for federal research grants, cooperative agreements, or SBIR/STTR contracts or grants. NRSICC would serve as the government's central point of contact to assist institutions that lack the capabilities and resources to conduct robust due diligence on their own.

The due diligence support efforts outlined in parts A and B can also inform and enhance the creation of a consolidated knowledge base on foreign entities posing national, economic, or ethical risks to the U.S. that the government currently lacks.

C. Research Security and Integrity Policy Development, Refinement

NRSICC will develop new government-wide policies on research security and integrity issues, including addressing the policy gaps described in this testimony. Through coordination with relevant agencies and White House offices, NRSICC would develop and design policies that would apply to all federal research grant awards and contracts in fundamental research domains. Policy development activity should include the following:

- Coordinate and implement all policy changes proposed at the interagency to be implemented by all federal funding agencies.

- Create or refine standardized application forms, periodic reports, and supporting documents on all federal research grants and SBIR/STTR awards.

- Track information on and develop new policies in response to China's integrity and reciprocity failures affecting federal research investments.

- Develop and refine due diligence and risk assessment methodologies and set standardized (government-wide) rules on federal award approval and denial decisions.

- Build a collection and analysis program to close persistent knowledge gaps on PRC entities that pose risks to US national interests and oversee the process for nominating entities that would be restricted. This effort would also include harmonizing the lists DoD is required to maintain with our export control and sanctions regimes.

- Develop and deploy training programs to build subject matter expertise among data analysts and risk assessors. Build separate (but related) training programs in coordination with NSF's OIG for investigators and prosecutors on how to conduct research grant and contract compliance investigations across the federal enterprise.

D. Cost Savings and Revenue Generation

- Consolidating all contracts, subscription services, and licenses into NRSICC, rather than having those duplicated across many federal funding agencies and research security offices, would save the government at least several million dollars annually.

- Initial automation and data aggregation tasks would save time and effort spent on initial due diligence, which would translate into potentially faster outputs and cost-savings through utilizing one IT infrastructure to produce and review materials.

- Incorporating the efforts of the newly established NSF SECURE Center[40] (Safeguarding the Entire Community of the U.S. Research Ecosystem) and its functions into the NRSICC will provide additional resources and could save taxpayer money.

- The increased civil grant compliance investigations, especially through False Claims Act litigation that result from dedicated NSRICC and investigative task force functions, would generate millions of dollars per year in recoveries from universities found liable and may cover most of the center's operating budget.

- Adding a 0.1% to 0.4% "due diligence tax" on all fundamental research grants and SBIR/STTR contracts would likely cover all costs associated with NRSICC's due diligence operations that support both federal agencies and research institutions requesting assistance.

NSRICC's functions and activities are partly intended to establish a genuine, whole-of-government approach to research security. The policies, subject matter expertise, and training programs developed by the center could also be used to support key allies and partners around the world that face many of the same threats and challenges from China as we do and, in many cases, have even fewer resources and capabilities to mitigate research security threats on their own.

[40] The current (nascent) tasks of NSF's SECURE Center, which is run by a consortium of universities, largely focus on awareness, training, and government-university engagements. Its functions are much more limited in scope than the proposed NRSICC.