U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
HEARING CHARTER

Balancing Open Science and Security in the U.S. Research Enterprise

Tuesday, October 5, 2021
10:00 am – 12:00 pm ET
Zoom

PURPOSE

The purpose of this hearing is to explore the risks to research integrity and security posed by undue foreign influence in the U.S. research enterprise. The Subcommittees will examine ongoing efforts at universities and federal science agencies to address these risks and the need for additional clarity regarding the scale and scope of the risks and best practices for securing federally funded fundamental research. They will also discuss the risks of overcorrection, including the impact on researchers, institutions, and the competitiveness of the U.S. research enterprise.

WITNESSES

- **Dr. Maria Zuber**, Co-Chair, National Science, Technology, and Security Roundtable, National Academies of Sciences, Engineering, and Medicine; Vice President for Research and E.A. Griswold Professor of Geophysics, Massachusetts Institute of Technology
- **Ms. Candice N. Wright**, Director, Science, Technology Assessment, and Analytics, U.S. Government Accountability Office
- **Ms. Allison Lerner**, Inspector General, National Science Foundation
- **Dr. Xiaoxing Xi**, Laura H. Carnell Professor of Physics, Temple University

KEY QUESTIONS

- What are the risks to the integrity and security of the U.S. research enterprise from undue foreign influence?
- How do agencies and universities work in collaboration with the intelligence community and law enforcement to identify and address research security risks? What are the challenges and successes of that partnership?
- What steps have agencies and universities taken to raise awareness and mitigate these risks? What does success look like? What are the goals agencies and universities are working toward?
- What are the potential risks of an overcorrection for continued U.S. leadership in science and innovation?

OPEN SCIENCE

Openness is one of the most important tenets of scientific research. Broad dissemination of results and data and the free exchange of ideas help facilitate wider evaluation and confirmation of results and spark new collaborations and avenues of inquiry. They increase the validity of research results, improve productivity and student training, and help deliver the benefits of research to the broader public. Openness also enables the scientific community to identify and correct for instances of scientific misconduct, such as fabrication or falsification of data, which enhances the integrity of the entire research enterprise and builds public trust.

While there are domains in which openness in science can be detrimental to national competitiveness or security, fundamental research has been generally exempted from security restrictions since 1985. President Reagan's National Security Decision Directive 189 (NSDD-189) defines fundamental research as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." It also dictates that "to the maximum extent possible, the products of fundamental research remain unrestricted," and specifies that "where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification."[1]

The directive does not claim that the open sharing of fundamental research is without risk. Rather, it asserts that openness in research is so important to competitiveness and security that it warrants the risk that adversaries may benefit from scientific openness as well. This principle was reaffirmed by Assistant to the President for National Security Affairs Condoleezza Rice in 2001[2] and by Undersecretary of Defense Ashton Carter in 2010.[3]

INTERNATIONAL COLLABORATION AND STUDENTS

The United States has benefitted greatly from international scientific collaboration and the contributions of foreign-born scientists. The COVID-19 pandemic has exemplified the value of working across borders to tackle global scientific challenges. Other complex and large-scale scientific endeavors, like the International Space Station[4], the Event Horizon Telescope[5], and the Large Hadron Collider[6] have required the pooling of resources, facilities, and expertise from multiple countries. These projects have enabled major scientific breakthroughs and, in many cases, have geopolitical benefits.

According to data collected by the National Science Foundation (NSF), the percentage of worldwide research articles produced with international collaboration increased from 17% to 23% between 2008 and 2018. In 1996, the United States' most common collaborator was the United Kingdom (13%). In 2018, it was China (26%), followed by the UK (13%), Germany (11%), and Canada (10%).[7] China is also the largest country of origin of international students in the United States.

[1] https://catalog.archives.gov/id/6879779
[2] https://sgp.fas.org/bush/cr110101.html
[3] https://www.acq.osd.mil/dpap/dars/pgi/docs/2012-D054%20Tab%20D%20OUSD%20(ATL)%20memorandum%20dated%20May%2024%202010.pdf
[4] https://www.nasa.gov/mission_pages/station/cooperation/index.html
[5] https://eventhorizontelescope.org/array
[6] https://home.cern/about/who-we-are/our-governance/member-states
[7] https://ncses.nsf.gov/pubs/nsb20206/international-collaboration

The United States attracts the largest share of internationally mobile students worldwide (19% in 2016). Temporary visa holders comprise a large proportion of science and engineering doctorate holders, including more than half of U.S. doctorate degrees awarded in engineering, computer science, and mathematics. Nearly three-quarters of these individuals remain working in the United States 10 years after receiving their degrees (72% in 2017).[8]

Since 2000, more than 38% of all U.S. Nobel laureates have been foreign-born, including more than 42% in physics, 35% in chemistry, and 32% in medicine.[9] As of 2018, 50 of the 91 privately held U.S. billion-dollar startup tech companies counted at least one immigrant among its founders. A quarter of those founders came to the United States as international students. These companies created an average of 1,200 jobs each and have a collective value of $250 billion.[10]

In recent years, universities have observed a significant decline in enrollment of international students. This trend accelerated dramatically last year due to the COVID-19 pandemic, with a 43% drop in enrollment in Fall 2020. Declines in previous years were more modest: 3.3% in 2016, 6.9% in 2017, and 0.9% in 2018 and 2019. These declines have been attributed to several factors, including visa application delays, increasing global competition for students, the social and political environment in the United States, and the costs of U.S. higher education.[11]

RESEARCH INTEGRITY AND SECURITY

Research integrity is a set of ethical standards that form the foundation for responsible conduct of research: objectivity, honesty, openness, accountability, fairness, and stewardship.[12] As a condition of receiving federal grant funds, scientists and research institutions must comply with agency grant requirements designed to protect the integrity of the science and prevent waste, fraud, and abuse of taxpayer funding. These include policies related to financial conflicts of interest (COI)[13], conflicts of commitment[14], and disclosure of researcher affiliations and other sources of support. Agencies award research grants to institutions, not researchers; therefore, institutions are primarily responsible for ensuring compliance with these policies.

When funding agencies become aware of an alleged instance of noncompliance through notification from the awardee institution, an anonymous tip, or another audit or investigation, they coordinate with the institution to assess the available evidence and determine if agency action is necessary. In many cases, an

[8] https://ncses.nsf.gov/pubs/nsb20198/immigration-and-the-s-e-workforce

[9] https://www.forbes.com/sites/stuartanderson/2020/10/14/immigrants-nobel-prizes-and-the-american-dream/?sh=3aee723c372e

[10] https://nfap.com/wp-content/uploads/2019/01/2018-BILLION-DOLLAR-STARTUPS.NFAP-Policy-Brief.2018-1.pdf

[11] https://www.iie.org/Research-and-Insights/Open-Doors/Fall-International-Enrollments-Snapshot-Reports

[12] https://www.nap.edu/catalog/21896/fostering-integrity-in-research

[13] OSTP defines "conflict of interest" as "a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research." https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[14] OSTP defines "conflict of commitment" as "a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many institutional policies define conflicts of commitment as conflicting commitments of time and effort, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share improperly information with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment." https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

agency works with the university and researcher to bring them into compliance and ensure expectations are made clear. If the agency suspects a researcher engaged in intentional deception, misconduct, or fraud, the agency can refer the case to the Office of the Inspector General (OIG) for further investigation. The OIG can and does initiate its own investigations as well. The OIG refers criminal cases to DOJ.

There is no consensus on the definition of "research security," but it is generally understood to encompass behavior that runs counter to U.S. science ethics as a result of undue foreign influence. While efforts by foreign entities to target U.S. intellectual capital have predominantly involved trade secret theft or violation of export control laws, this hearing is primarily focused on risks to federally funded fundamental research at universities. Funding agencies and DOJ have identified and cracked down on a number of specific behaviors:

- failure to disclose conflicts of financial and non-financial interest, including funding, parallel laboratories, employment, affiliations, and appointments;
- failure by peer reviewers to keep information in grant applications confidential, including disclosure to foreign entities or other attempts to influence funding decisions; and
- diversion of intellectual property in grant applications or produced by agency-supported research to other entities, including other countries.

Such behaviors can compromise the integrity of the research and, in some cases, undermine economic competitiveness or national security interests. The Chinese government is not unique in engaging in influence in the U.S. research enterprise, but it appears to be the most active and best organized. Talent recruitment programs sponsored by the Chinese government, most notably the Thousand Talents Plan, have been a major source of concern. Foreign talent recruitment programs are not new and are not unique to China. They are an effort by a foreign government to recruit science and technology professionals or students to advance that country's economic development and/or national security goals. Participation in a foreign talent recruitment program does not necessarily warrant suspicion of improper behavior. However, in recent years, research funding agencies have uncovered a correlation between noncompliance with COI and disclosure requirements and participation in Chinese-government sponsored talent recruitment programs. In fact, some Chinese talent recruitment program contracts contain provisions that encourage or require such behavior.[15,16] Heightened concerns about risks to research security have spurred a flurry of action by research funding agencies and the Department of Justice (DOJ) in recent years.

RECENT ACTIONS

Reports and Guidance Documents

In the last few years, multiple government entities have written or commissioned guidance documents in an attempt to define known threats to the U.S. research enterprise.

In December 2019, JASON issued an NSF-commissioned report titled "Fundamental Research Security".[17] JASON is an independent science advisory group that contracts with government agencies to produce

[15] https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf

[16] https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise-June-2020.pdf

[17] https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

reports on matters of defense science and technology.[18] The report affirmed the importance of foreign scientific talent, warned against placing new restrictions on access to fundamental research, and acknowledged the difficulty in assessing the scale and scope of legitimate threats to research security. The JASONs concluded "many of the problems of foreign influence that have been identified are ones that can be addressed within the framework of research integrity."

GAO issued a report in December 2020 assessing the COI and disclosure policies at NSF, NIH, the National Aeronautics and Space Administration (NASA), the Department of Defense (DOD), the Department of Energy (DOE), and 11 universities.[19] GAO found that all five agencies require researchers to disclose information as part of their grant proposal but that there was variability in the policies and agencies lack clear enforcement mechanisms. GAO also concluded that, due to differing policies and inconsistent implementation, researchers may be unsure of what they need to disclose.

In response to congressional direction[20], the National Science and Technology Council (NSTC) Joint Committee on the Research Environment (JCORE) issued a report in January 2021 titled "Recommended Practices for Strengthening the Security and Integrity of America's S&T Research Enterprise."[21] It was prepared in coordination with the National Security Council and complements the National Security Presidential Memorandum 33 (NSPM-33)[22], which creates disclosure requirements for R&D funding and directs the coordination of policies among stakeholders across the Federal government.[23] NSPM-33 directs actions by funding agencies to secure intellectual capital while acknowledging the importance of openness and scientific collaboration. These include:

- prohibiting Federal personnel from participating in foreign-government-sponsored talent recruitment programs;
- requiring institutions to develop research security programs;
- directing agencies and universities to share information about individuals whose behavior poses a risk to research integrity and security;
- directing the Department of State and the Department of Homeland Security to review vetting processes for foreign students and researchers;
- directing agencies to harmonize disclosure processes and definitions; and
- streamlining the grant application process through the use of digital persistent identifiers (DPI).

While the university and research community welcomed the release of NSPM-33, many called for additional clarity on implementation and an opportunity to provide input.[24, 25] Last month, OSTP Director Eric Lander issued a press release announcing OSTP's intent to develop implementation guidance for federal agencies to address disclosure policies, oversight and enforcement of violations, and research security programs for organizations that receive over $50 million in annual R&D funding.[26]

[18] https://irp.fas.org/agency/dod/jason/
[19] https://www.gao.gov/assets/gao-21-130.pdf
[20] https://www.congress.gov/bill/116th-congress/senate-bill/1790
[21] https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf
[22] https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/
[23] https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSC-OSTP-NSPM33-Fact-Sheet-Jan2021.pdf
[24] https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/JCORE.Recs-%20Assn.%20Memo.Final.pdf
[25] https://www.aps.org/about/governance/letters/upload/APS-Letter-NSPM33-March2021.pdf
[26] https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/

Research Funding Agencies

NSF has taken a number of steps to address research security risks. In July 2019, NSF issued a policy prohibiting NSF employees and rotators from participating in foreign talent recruitment programs.[27] In February 2020, NSF clarified that its disclosure requirement for grant applicants includes both foreign and domestic sources of support.[28] In March 2020, NSF established a new Chief of Research Security Strategy and Policy position.[29] In September 2021, in partnership with NIH, NSF implemented a new digital format for submitting researcher biographical sketches as part of grant applications to simplify and standardize the disclosure process for researchers seeking funding from both agencies.[30]

NIH also issued a reminder to the research community of their full disclosure requirements.[31] NIH established a Working Group on Foreign Influence on Research Integrity, which released a December 2018 report with recommendations for NIH and universities on raising awareness of foreign influence and safeguarding research integrity.[32] In 2020, NIH issued policies and provided internal training to protect confidentiality in the peer review process.[33, 34, 35]

DOE issued a memo in December 2018 affirming the importance of research collaboration but raising alarms about foreign influence. The memo established a DOE S&T Risk Matrix, which identifies emerging research areas and technologies subject to restricted access by and collaboration with "sensitive country foreign nationals". The Risk Matrix is being used by the agency but is not publicly accessible. DOE also set up a Federal Oversight Advisory Body (FOAB) to maintain the Risk Matrix and process exemption requests.[36] In June 2019, DOE issued a directive prohibiting DOE employees and contractors from participating in foreign talent recruitment programs sponsored by China, Iran, North Korea, and Russia.[37]

Universities

The capacity to respond to research security risks varies depending on the resources, staffing, and expertise available at each institution. Some universities have set up new research security programs dedicated to identifying and mitigating risks in coordination with the IC, law enforcement, and research funding agencies. Smaller institutions are focused on raising awareness and keeping up with the patchwork of new requirements. A fall 2019 survey describes the range of activities on university campuses.[38]

[27] https://www.nsf.gov/bfa/dias/policy/researchprotection/PersonnelPolicyForeignGovTalentRecruitment%20Programs07_11_2019.pdf

[28] https://nsfpolicyoutreach.com/resources/2-20-pappg-webinar/

[29] https://www.nsf.gov/news/news_summ.jsp?cntn_id=300086

[30] https://www.nsf.gov/bfa/dias/policy/biosketch.jsp

[31] https://grants.nih.gov/grants/guide/notice-files/NOT-OD-18-160.html

[32] https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf

[33] https://www.csr.nih.gov/RevTrainingPubRevNoSurvey/Home

[34] https://www.youtube.com/watch?v=X0yvzUUc9yY

[35] https://grants.nih.gov/grants/guide/notice-files/NOT-OD-21-019.html

[36] https://www.aplu.org/members/councils/governmental-affairs/cga-miscellaneous-documents/DOE%20Memo%20Dec%2014%202018.pdf

[37] https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder

[38] https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf

DOJ China Initiative

In November 2018, the Trump administration established the China Initiative under the DOJ's National Security Division. The stated goals of the Initiative were to identify and investigate trade secret theft cases from nontraditional collectors, namely "researchers in labs, universities and the defense industrial base."[39] On its website, the China Initiative lists 89 "China-related cases examples," some preceding the establishment of the Initiative and at least one – the arrest of Dr. Anming Hu – referencing a defendant who has been acquitted of all charges.[40] A 2020 FBI press release points to three guilty pleas under the Initiative in the 2019-2020 year, and ten academics charged in total.[41] The China Initiative remains active under the Biden Administration. No new case examples have been added to the website since May 2021.

CONTINUING CHALLENGES

The Scale of the Problem

More than three years after concerns were initially raised, the precise scale and scope of research security risks are still not known by the government. The uncertainty about the fraction of federally funded researchers engaged in illicit behavior makes it difficult to track trends over time and impossible to assess the success of mitigation measures. The university community has even less access to information because it is either classified or withheld for privacy reasons. The lack of data and information sharing – beyond anecdotes - has impeded efforts to bring university administrators and researchers up to speed regarding the risk landscape and to build a sense of shared responsibility throughout the scientific community.

Culture Clash

Cultural differences between academics and the intelligence community (IC) and law enforcement are another major challenge. The IC and law enforcement are faced with the challenging task of communicating a diffuse and rapidly evolving threat to a large and, at times, unreceptive audience. The IC and law enforcement generally prioritize mitigating that threat, while researchers tend to prioritize ensuring science remains open and as unencumbered as possible. There is also a deficit of technical expertise within the IC and law enforcement, which has led to instances of prosecution based on a misunderstanding of the technology in question and academic norms. While progress has been made in bridging these divides, there is still a sense of frustration and feeling misunderstood on both sides.

Racial Profiling

Entities looking to protect U.S. research from theft have largely focused on China, leading to concerns about racial profiling of scientists of Chinese and East Asian heritage. The Committee of 100, a leadership organization of Chinese Americans, recently published a report analyzing cases charged under the Economic Espionage Act (EEA) from 1996 to 2020.[42] The report found that defendants with Chinese last names comprised 57 percent of EEA cases from 2009-2016 and 52 percent of cases from 2017-2020 – a stark increase from 16 percent in 1996-2008. Defendants with Chinese surnames who were convicted were sentenced to an average of 27 months in prison, compared to an average of 12 months for defendants with

[39] https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

[40] https://www.knoxnews.com/story/news/2021/09/09/tennessee-professor-hu-acquitted-spying-charges/8265020002/

[41] https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20

[42] https://www.committee100.org/wp-content/uploads/2021/09/Whitepaper-Final-9.21-UPDATE-compressed.pdf

Western names. Strikingly, the rate of Chinese surnamed defendants who were charged but never convicted – 22 percent – was twice the rate of Western surnamed defendants.

Many academic societies and Asian American advocacy groups have raised the alarm about racial profiling in the research security space. Many of the highest[43] profile[44] economic espionage cases[45] tied to China have focused on academics, despite research institutions only comprising 3 percent of all EEA cases.[46] Asian Americans Advancing Justice led a letter from advocacy groups and Asian-American individuals to then-President-Elect Biden decrying the "wrongful prosecutions of Asian American scientists" and asking him to end the China Initiative.[47] This month, the American Physical Society recommended Attorney General Merrick Garland and OSTP Director Lander reformulate the China Initiative to cede research integrity issues – such as failure to disclose foreign ties – to institutions and funding agencies, rather than the DOJ, due to false allegations and unfair targeting of scientists of Asian descent.[48]

University Cybersecurity

Universities are increasingly the target of cyber-attacks by both cybercriminals and nation state actors to obtain sensitive information and prepublication research. For example, the University of California, San Francisco, paid $1.1 million to criminals ransoming sensitive data in June 2020.[49] Moreover, with researchers and students working from home during the pandemic, the large number of personal devices connecting to institutional networks has increased the threat of attack. Academia largely functions through the free exchange of information, with open technology environments for collaboration. University cybersecurity budgets are also tight. As a result, many universities are both unwilling to adopt restrictive security practices and ill-equipped to follow resource-intensive standards to protect sensitive information. Cybersecurity is an important source of vulnerability that foreign governments have attempted to exploit, but it has not been a central focus of efforts to address research security risks to date.

[43] https://www.knoxnews.com/story/news/2021/09/09/tennessee-professor-hu-acquitted-spying-charges/8265020002/

[44] https://www.nytimes.com/2015/09/12/us/politics/us-drops-charges-that-professor-shared-technology-with-china.html

[45] https://www.nytimes.com/2015/05/10/business/accused-of-spying-for-china-until-she-wasnt.html

[46] https://www.committee100.org/wp-content/uploads/2021/09/Whitepaper-Final-9.21-UPDATE-compressed.pdf

[47] https://advancingjustice-aajc.org/sites/default/files/2021-01/Letter%20to%20President-elect%20Biden%20Re%20the%20China%20Initiative.pdf

[48] https://www.aps.org/policy/analysis/upload/APS_Letter_China_Initiative_Sept_2021.pdf

[49] https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=59a3a5ab18a8