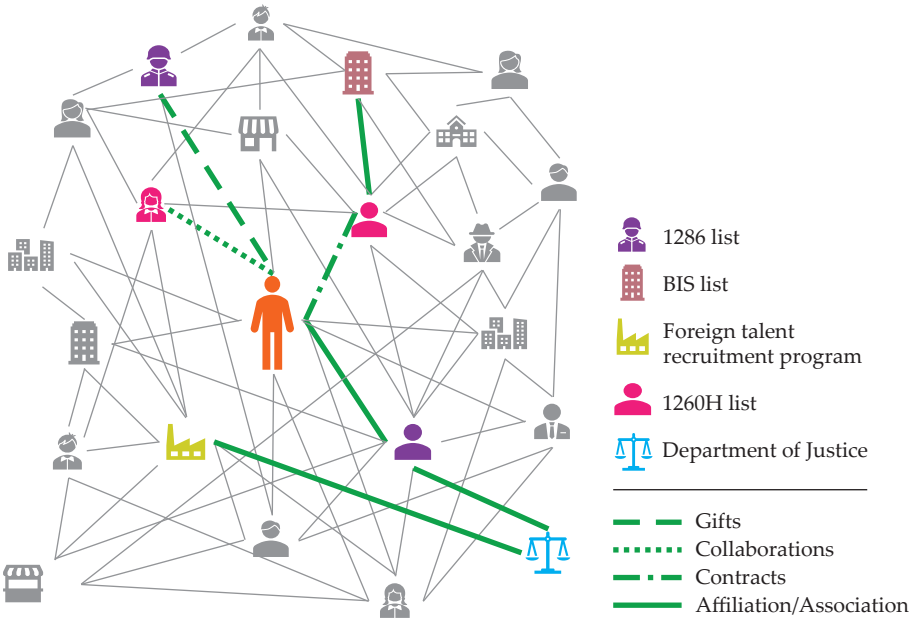
US research enterprise seeks to retain leadership while upping security

Uncertainty shrouds research-security measures and how to comply with them.

The vetting of US scientists and their work by the federal government for potential foreign influence concerns—willful or otherwise—for decades was mostly limited to research with near-term national security or commercial implications. Now, scrutiny is starting to be applied more broadly and more strictly. Connections with China are especially under the microscope.

The aim of increased scrutiny, explains Tam Dao, associate vice president of campus safety and research security at Rice University, is to ensure that international collaborations are transparent, ethical, and mutually beneficial. Research-security officials support researchers in "assessing potential risks of undue foreign influence," he says. "We work hard on early intervention and education. We are not waiting for someone to do something bad and then nail them." International collaboration, he adds, "is critical to research success."

Scientific collaborations between the US and China have skyrocketed, notes Caroline Wagner, a professor of public policy at the Ohio State University who studies international collaborations. In the early 2000s, she says, 2–3% of US international collaborations were with China; by early this decade, it was 20–25%. A very small number of researchers in the US system are "bad actors," she says. "My real concern about the tightened measures is the harm it could do to US science and technology—both reputationally and in the sense of knowledge-creation opportunities that could evaporate under enhanced scrutiny."



ASSESSING THE CONNECTIONS of researchers applying for grants is part of research-security efforts. Ties to people and institutions that are on various US government lists can lead to requests for mitigation measures, including severing ties, for funding to be approved. In this diagram, a hypothetical principal investigator (center, orange) is revealed to have connections with various entities of concern. The Department of Defense's 1286 list includes foreign institutions that the department says are engaging in activities related to technology transfer and talent recruitment that threaten national security; the 1260H list highlights Chinese military companies operating in the US; the Bureau of Industry and Security (BIS) list contains names of businesses, research institutions, government and private organizations, and individuals that are subject to federal licensing requirements; and foreign talent recruitment programs targeting science and technology professionals and students can lead to conflicts of commitment. The Department of Justice generally oversees research-security transgressions. (Figure adapted from an image provided by Tam K. Dao/Rice University.)

Directives

The turning point for tightening research security came nearly a decade ago, says Dao, who back then was a Federal Bureau of Investigation special agent focusing on economic-espionage investigations. "Intelligence agencies started to share materials with federal funding agencies to inform them there were issues with undue foreign influence," he says. Since then, government entities have picked up the pace in defining, tightening, and increasing enforcement of research-security measures.

In 2019, JASON, a group of scientists that advises the government on sensitive science and technology issues, provided NSF with recommendations on research security. In a March 2024 update, JASON noted that "recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC."

In January 2021, President Trump issued a memorandum directing the strengthening of protections for US-

RESEARCH-SECURITY OFFICERS from around the country identify needs they'd like to see addressed by the new SECURE (Safeguarding the Entire Community of the U.S. Research Ecosystem) center. The exercise took place in February at a conference of the Academic Security and Counter Exploitation program in College Station, Texas. (Photo courtesy of Mark Haselkorn.)

government supported R&D "against foreign government interference and exploitation." The following year, the CHIPS and Science Act codified into law the memorandum's requirements for research-security provisions and included directives intended to protect US commercial and national security interests and to help with their implementation.

Universities want to comply with the security requirements, says an administrator at a large public university who requested anonymity. "But it's complicated. And the consequences of failing to comply are substantial." Last year, for example, the US government filed suit against Georgia Tech for allegedly violating cybersecurity regulations.

"We fret about increased costs to comply in a time when funding may shrink due to outright cuts and to reduced overhead funds," the administrator says. Extra costs could come, for example, from requirements to mandate training, fill out forms, cordon off areas for confidential unclassified work, and maintain separate, secure computer systems.

For many university faculty members, details about the implementation of research-security measures remain fuzzy. And uncertainty both about what is permitted and how the measures play out has cast a chill over research communities.

The requirements "are a moving target," says Kenny Evans, who studies research security at Rice University's Baker Institute for Public Policy. "There is a ton of confusion about what constitutes risk." The US government has designated China, Iran, North Korea, and Russia "countries of concern." Yet for the past few decades, the US has benefitted from attracting large numbers of international graduate students, including ones from those countries.

The theft of intellectual property and technology does happen. Michael Shannon was a longtime government investigator and since 2022 has been at IPTalons, a startup that offers services in research-security risk assessment. Shannon estimates from company data that 95% of US-funded researchers have international connections and that 75–80% of them have failed to report something. Most of the omissions are paperwork violations that can be fixed, he says, but 3–5% are "deliberate."

Many US researchers acknowledge that increased security measures are needed. But such measures "have to be applied carefully so as not to hurt the competitiveness of US science and scientists," cautions a physics professor originally from China whose institution requested anonymity because of the topic's sensitivity. Many researchers worry that the US is, as Evans puts it, "fueling China's abilities" by pushing people out and that the blanket application of increased security measures could compromise US standing in science.

Risks and reactions

A major challenge, the university administrator says, "is the lack of harmonization between agencies." The Department of Defense, for example, has well-established research-security measures. The same goes for the Department of Energy weapons labs and other funders. But the measures differ from agency to agency.

Complicating matters is that some states are superimposing their own security measures on research. And faculty members are accustomed to independence. "They value open science and have not seen sharing information as a threat," the administrator says.

At many institutions, researchers must file annual disclosures that include names of collaborating scientists and their affiliations, past and planned travel, monetary gifts and sources of funding, and potential conflicts of interest. Researchers provide similar information when they apply for grants from federal agencies. In the past, institutions could

TAM DAO, associate vice president of campus safety and research security at Rice University, addresses participants at the first global workshop on "research on research security," held at Rice in May 2024. (Photo from Michael Stravato, Baker Institute for Public Policy, Rice University.)

say they were in legal compliance as long as they had collected the requested information, Shannon says, but "nowhere in the oversight process was the veracity checked." That's changing.

When disclosures raise flags, Dao says, his job is to provide researchers with accurate information about agency rules so they can make an informed decision through the lens of national security. A researcher's decision could boil down to implementing mitigation measures or forgoing funding. Mitigation might include taking additional research-security training, ceasing a particular collaboration, refusing money or travel perks from some foreign source, or meeting with counterintelligence representatives from the funding agency. Getting flagged is common, Dao says. The agencies, he adds, "have made it clear that their goal is to get to 'yes.' "

Still, many researchers find the increased scrutiny cumbersome and even scary. Some Chinese-origin faculty members say they have stopped applying for grants from the US government. And many researchers have minimized or discontinued their professional connections with colleagues in China.

While on a personal trip to China in 2023, the physics professor whose institution asked not to be identified was invited to give an academic talk at a university in Shanghai. The professor paid out of pocket for local travel and lodging to avoid having to explain—to their institution and funding agencies—accepting money from a Chinese entity. As a precaution, the professor has also stopped collaborating with Chinese colleagues—often former postdocs or graduate students. "I won't publish with colleagues if they include an affiliation in China," they say. "That is a loss for me as a researcher. The reduced collaborations in fundamental science between the two countries is a huge loss for the whole scientific community."

Peter Littlewood, a physicist at the University of Chicago and former director of Argonne National Laboratory, says that "it's not regarded as a conflict of interest" when an institution in the US pays his travel expenses to give a seminar. But when traveling to a country of concern, the same behavior "is treated differently." A few years ago, he says, he "got the message" to reduce travel to China. DOE officials "didn't say don't go," he says. "But the number of questions you had to answer was growing, and they made it clear you'd save the legal department a lot of time if you did not travel to China."

Condensed-matter theorist Steven Kivelson of Stanford University says he jumped through hoops to get funding to attend a conference in China last fall. A non-Chinese US scientist who requested anonymity says they no longer respond to emails from China because they "don't want to be flagged as a risk." And many scientists express worry that US faculty members will become hesitant to take on students from China and other countries of concern because of the difficulties that future collaborations may bring.

New measures, long-term effects

Last summer, NSF announced a pilot program called Trusted Research Using Safeguards and Transparency. Initially limited to quantum-related studies, TRUST applies an extra layer of scrutiny to proposals that receive high rankings from peer reviewers. NSF wouldn't say what that scrutiny involves, although a spokesperson wrote that "the TRUST process has no implications for the nationality of who can work on quantum-related projects funded by NSF."

Rice's Dao says, "We don't know the details except that [NSF] will likely assess active appointments, positions, research support, and instances of nondisclosure." In any case, says Sophia

Economou, director of Virginia Tech's Center for Quantum Information Science and Engineering, the extra scrutiny will cause delays. "That could lead to big gaps in funding and can affect younger faculty who have the pressure of the tenure clock," she says. "I worry about them."

Another new research-security measure stems from the National Defense Authorization Act (NDAA) that was signed into law last year. It bars scientists who are from the four countries of concern and don't have US resident status from working at the National Nuclear Security Administration (NNSA) labs. Foreign nationals at those sites work on unclassified, often fundamental science.

In February, around 60 non-US citizens, mostly from China, lost access to the campus of Lawrence Livermore National Laboratory, one of the three NNSA labs. They now spend workdays in a building off-site. One of them is a physicist who has been at Livermore for several years. That physicist says they can still run simulations and analyze data, but some other scientists lack the apparatuses necessary to continue experiments. The physicist says they feel isolated and uncertain about their future; they asked not to be identified because they fear retribution and hope to find either a solution at Livermore or other employment in the US.

The physicist and others also question the necessity of the exclusion. The security checks and rules for working at the NNSA labs are extensive. For example, says the physicist, "There are specific computers I am allowed to touch, and I am not the administrator of my own computer." Sometimes their students' computers were off-limits, they add.

Shutting out Chinese and other foreign researchers "is a move in the wrong direction," says Siegfried Hecker, who was director of Los Alamos National Laboratory from 1986 to 1997. The law specifies that waivers are possible but, he says, "the way the government works, that never happens." To stay "at the top of the game," he adds, "you have to attract the smartest people. Then you have to manage risk. And places like Los Alamos know how to do security."

"The effects of the NDAA changes will have a long lead time to understand how devastating they will be," says Hecker. "With research security, it will be years before we understand the harm to US science."

Spokespeople from the nation's three NNSA labs said only that the labs are complying with the NDAA. They did not respond to questions about how many people are affected or how the loss of those scientists affects the labs' research.

New center serves as liaison

To help bolster research security, the CHIPS and Science Act calls for measures to aid in implementation. The 400 or so universities that receive more than $50 million annually from the federal government are now required to set up research-security offices. (Several universities are creating master's degree programs to prepare people for careers in those offices.)

And an NSF-backed program, Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE), is ramping up to serve as a bridge between government funding agencies and the research community. Funded through the CHIPS and Science Act with $67 million over five years, SECURE encompasses a center headquartered at the University of Washington and one focused on analytics led by Texas A&M. The aim, says UW center director Mark Haselkorn, is to enable researchers and research administrators "to be secure and to protect the value of what they create while also sustaining the collaborative open environments in which research thrives."

Working with the research community, the SECURE team has come up with priorities that include providing tools to interpret and navigate research-security policies, reducing the burden of agencies' various security requirements for researchers, and developing guidance for managing foreign travel. This summer, Haselkorn says, the center will roll out a virtual environment where researchers and research-security officers can share information. The center is also creating a condensed version of a research-security training course that will satisfy requirements for all federal funding agencies.

"SECURE will do a service by making it clear what's in and what's out," says Ohio State's Wagner, leader of the new center's evaluation team. "That could make people less fearful about collaborations."

Toni Feder