SAFEGUARDING ACADEMIA

Protecting Fundamental Research, Intellectual Property, Critical Technologies, and the U.S. Research Ecosystem

NCSC

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NSF

About NCSC

A component of the Office of the Director of National Intelligence (ODNI), the National Counterintelligence and Security Center (NCSC) leads the nation's counterintelligence (CI) and security efforts by providing CI and security expertise, guidance, and support to the U.S. Intelligence Community and other stakeholders. Through its outreach efforts, NCSC engages with government agencies, industry partners, and academia to raise awareness about CI and security threats, promote best practices, and foster collaboration to protect the nation's security and advance U.S. interests. This bulletin represents a collaborative effort across NCSC's stakeholder community.

Table of Contents

01

Overview

02

Risk Environment

04 Targeting Emerging Technology, Research, & Talent

07 Talent Poaching

08 Foreign Talent Recruitment Programs

13 Foreign Research Collaboration

14 Targeting Students for Potential Recruitment to Conduct Espionage

16

Impact

17

Indicators

Elicitation 18

Insider Threats & Access 20

Cyber Intrusions & Social Media 20

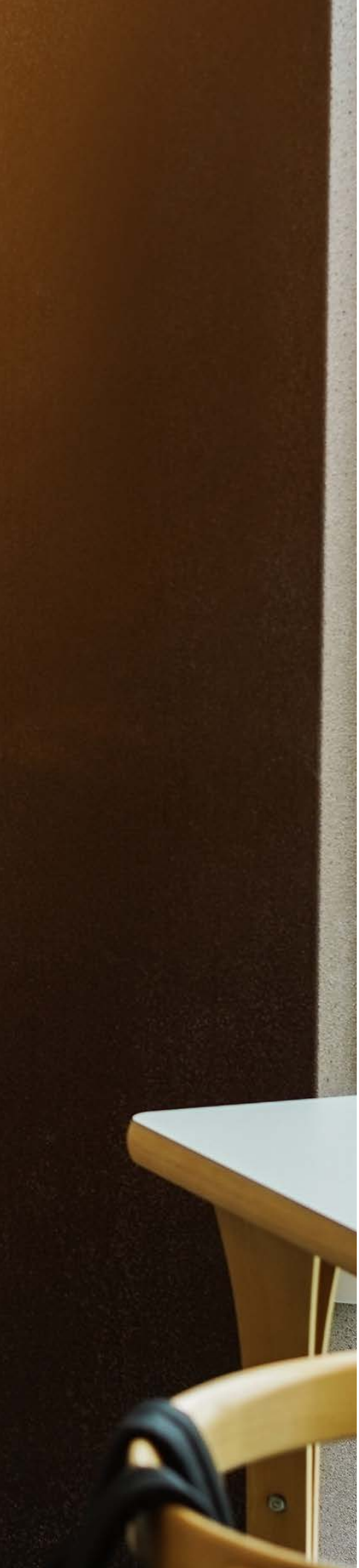
23

Mitigations

28 Additional Resources

31

Reporting



Safeguarding Academia

The United States (U.S.) values international collaboration as a cornerstone of academic excellence. Engaging with our global academic partners enhances the quality of research, drives scientific discovery, and fosters innovation.

At the same time, it is important that the U.S. academic community understand the increasing risks posed by foreign adversaries, specifically foreign intelligence entities and their proxies, who continue to exploit the open nature of U.S. institutions of higher education to acquire scientific and technical information to advance their own technological and innovation goals. Protecting the integrity of U.S. research—while fostering international collaboration—is critical to maintaining a robust and secure research ecosystem. Striking this balance is essential to preserving academic freedom, safeguarding researchers' lifework, and ensuring that innovation continues to thrive in a secure and principled manner.

This bulletin provides guidance for the U.S. academic community to promote a research ecosystem that balances openness, collaboration, integrity, fairness, responsibility, and security. By fostering a culture of scientific stewardship and heightened security awareness, the U.S. can better protect its scientific enterprise while sustaining its global leadership in innovation.

Risk Environment

Foreign adversaries use a variety of methods—such as theft, plagiarism, talent recruitment, cyber intrusions, elicitation, and the manipulation of collaborative research programs—to acquire research and advance their own academic and nation-state goals. In doing so, they diminish the U.S. academic environment and the overall innovation ecosystem that supports U.S. research.

Safeguarding science requires cultivating a research ecosystem that not only fosters innovation through collaboration, openness, and integrity, but also prioritizes security. An informed and empowered scientific community is best equipped to responsibly assess emerging technologies, anticipate their potential misuse, and implement protective measures.

Targets of foreign adversaries within academia may include:

- Individuals (e.g., students, faculty, researchers, administrators) with access to research and technical information
- Pre-publication research results and data
- Proprietary techniques and processes
- Research and laboratory procedures
- Practical knowledge and technical expertise
- Laboratory equipment, software, and computing resources
- Physical and virtual access protocols and passwords
- Budget estimates and grant information
- Prototypes or blueprints
- Student, employee, customer, or U.S. person data

The next section of this document highlights activities and potential indicators that may be used by foreign intelligence entities and their proxies, including non-traditional collectors, to exploit students and research at U.S. academic institutions.

Consider:

- → *Are there any potential ethical or moral concerns related to the application of your research?*
- → *Could your research be used to support activities in other countries with ethical standards incompatible with our own, such as internal surveillance and repression?*
- → *Are there any dual-use (both military and non-military) applications to your research?*
- → *Could your research benefit a foreign state's military, be supplied to other foreign state actors, or be exploited by a criminal enterprise?*
- → *Is any of your research likely to be subject to U.S. export controls?*
- → *Is your research likely to have a commercial or patentable outcome from which you or your organization would want to benefit?*
- → *Do you need to protect sensitive data or personally identifiable information? This may include genetic or medical information, population datasets, details of individuals, or commercial test data.*

Targeting Emerging Technology, Research, & Talent

Foreign intelligence targeting of scientific research at U.S. academic institutions—particularly of emerging technologies—is one of the primary counterintelligence threats we see today. U.S. adversaries are laser-focused on the economic and military benefits of these technologies, as they seek to acquire the research, innovation, and talent behind them.

Some nations have enacted comprehensive national strategies to achieve technological leadership. Russia and other countries, for example, target technology sectors to advance their own programs. But no nation has targeted Western research, science, and technology as aggressively as China. The Chinese Communist Party (CCP) and Chinese intelligence services represent the broadest, most active, and persistent espionage threat to the U.S. It also remains the top threat to U.S. technology competitiveness. China continues to target and attempt to acquire all manner of critical and enabling U.S. technologies, particularly electronics, software, communications equipment, and other materials to advance their economic and military objectives. Additionally, it attempts to recruit U.S. subject matter experts in critical and emerging technology fields, such as artificial intelligence/machine learning (AI/ML), quantum technologies, semiconductors, optics, hypersonics, and energy systems.

The U.S. academic community carries out research to advance human knowledge and serve the greater good. However, not everyone shares these noble intentions. China and other foreign threat actors exploit research in fields such as genetics, medicine, AI/ML, and more to suppress vulnerable populations and target individuals. Robust research security practices are key to ensuring cutting-edge research is not misappropriated and misused to cause harm. As an example of the harm this can cause, a professor at a U.S. university shared genetic data with Chinese researchers that was subsequently used by China's Ministry of Public Security to profile and surveil the Uighur population, a predominantly Muslim ethnic minority. The data was used to build a comprehensive DNA database that enabled the CCP to identify and track Uighur dissidents, sparking widespread criticism from human rights groups. This case underscores the need for researchers, institutions, and governments to work together to establish robust safeguards and due diligence practices to prevent the misuse of research and protect against foreign malign influence.

It is important to emphasize that the concern lies with China's government, the CCP, and its intelligence services, not the Chinese people or Chinese Americans who are often victimized by China. We continue to see repressive foreign regimes and their proxies target foreign students on U.S. campuses who speak out about abuses by their home governments. This is called transnational repression. These students are targeted for merely exercising their fundamental rights to free speech in the United States. To learn more about transnational repression at U.S. colleges and universities, see "Foreign Malign Influence and Higher Education" on the FBI website.

CASE STUDY

Transnational Repression

In April 2024, a student from China studying at a music college in Boston was sentenced to nine months in prison for stalking and threatening a fellow Chinese student who posted campus fliers supporting democracy in China.

The perpetrator threatened to chop off the victim's hands for posting the fliers and alert China's security services so they could target her family in China.

CASE STUDY

Talent Poaching

- A South Korean consulting firm recently broadcast a talent search for U.S. semiconductor experts to work for unspecified clients and offered compensation upwards of $300 per hour. Subsequent review revealed that the consulting firm was a front company for China's People's Liberation Army.
- In another case, a government-backed talent recruitment center in China solicited an advanced manufacturing materials expert at a U.S. Government laboratory. The center offered subsidized housing, free education for family members, and dedicated research funding of $550,000 per year to advance China's national technology development strategies.
- An East Asia and Pacific region consulting firm attempted to recruit cleared defense contractor employees with notable achievements in science and engineering in conjunction with a talent recruitment plan designed to facilitate technology transfer to advance their scientific, economic, and military development goals. The recruitment attempts advertised expedited visa services, annual salary, living accommodations, project funding, post-retirement welfare benefits, and school placement for researchers with children.

Talent Poaching

Foreign threat actors continue to aggressively recruit and successfully poach experts in AI, semiconductor, quantum, biotechnology, and other advanced technologies from our research ecosystem to advance their own scientific, economic, and military development programs. By doing so, they can save their countries significant time, money, and resources while achieving generational advances in technology.

Increasingly, the competition for global technology is a competition for talent. Adversaries understand that acquiring top talent can be more valuable than acquiring the technology itself.

When leading experts, researchers, and graduates take their skills abroad—especially to nations that may not algin with U.S. interests—it can accelerate the development of technologies that could ultimately be used against us. Faculty and researchers entrusted with cutting-edge projects funded by government and private sectors are key to this issue. Their collaboration with or relocation to foreign adversaries risks the loss of sensitive knowledge and endangers U.S. national security.

Moreover, foreign recruitment often involves the manipulation of U.S. students, faculty, and researchers, luring them with promises of resources, funding, or opportunities. However, these talents could find their work co-opted and potentially misused by authoritarian governments for purposes that contradict the principles of academic freedom, human rights, or global peace. Innovations meant to advance the public good may instead be diverted to harmful agendas.

In addition, foreign recruitment of U.S. talent undermines the innovation driven by our universities, which fuels the U.S. economy. As these individuals are drawn abroad, the U.S. loses the potential to create new industries, competitive companies, and high-paying jobs. Innovations that could have boosted domestic growth instead benefit foreign countries, widening the economic gap.

The choice of where to apply one's talent—whether as a student, faculty member, researcher, or administrator—carries implications beyond personal careers. It impacts the entire economic ecosystem, the future of our nation, and the preservation of our values. Consistent recruitment of top talent by foreign adversaries could reduce U.S. global leadership in education, innovation, and security.

Continuing to contribute skills to U.S. institutions helps sustain an environment where American values, security, and competitiveness thrive. This is not just about preventing loss; it is about actively contributing to a brighter future for the U.S. and the world—ensuring that scientific progress serves the common good, not the narrow aims of authoritarian regimes.

Foreign Talent Recruitment Programs

Foreign talent recruitment programs can threaten U.S. national security and research integrity. A foreign talent recruitment program is an effort directly or indirectly organized, managed, or funded by a foreign government or institution to recruit science and technology professionals or students (regardless of citizenship or national origin, and whether they have a full-time or part-time position). Association with talent recruitment plans by itself is not illegal; however, potential participants and their employers should be aware of legal issues that may arise as a result of participation, including violation of export-control laws, economic espionage, or violation of conflict-of-interest policies. These programs can lead to conflicts of interest, conflicts of commitment, intellectual property theft, and the transfer of U.S. federally funded research to foreign governments. They frequently involve the unauthorized transfer of research materials, data, or other non-public information, and can lead to conflicting obligations between multiple employers or entities.

Even if talent plan participants who steal information are eventually caught and prosecuted, the damage done to institutions by intellectual property theft may be irreversible. Additionally, though association with talent plans is not inherently illegal, failure to disclose affiliations with these plans may violate U.S. law and create risk of criminal prosecution for intellectual property theft or the misuse of grant funds. Talent plan participants have pleaded guilty to, or been convicted of, offenses including:

- Export-control law violations
- Economic espionage and theft of trade secrets
- Grant and tax fraud

Participation in a federally-funded research and development project may also be contingent on non-participation in a malign foreign talent recruitment program. It is therefore important for individuals to be familiar with, and abide by, disclosure and conflict-of-interest rules required by institutions and the U.S. Government. Transparency and full disclosure of talent plan membership and foreign contracts or agreements are essential for institutions to assess risk.

Foreign Talent Recruitment

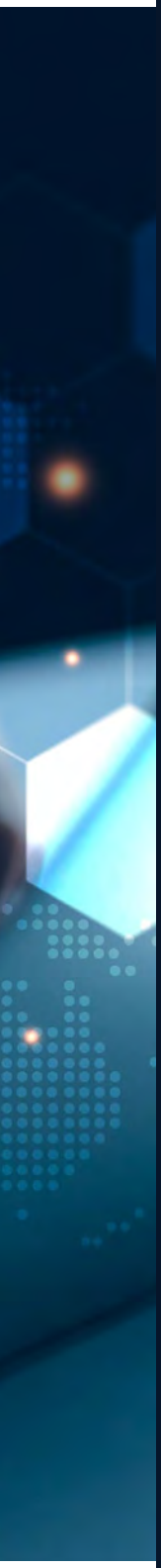
In 2020, James Patrick Lewis, pleaded guilty to one count of federal program fraud. From 2006 to August 2019, Lewis was a tenured professor at West Virginia University (WVU) in the physics department, specializing in molecular reactions used in coal conversion technologies. In July 2017, Lewis entered a contract of employment with China through its "Global Experts 1000 Talents Plan." China's Thousand Talents Plan was one of the most prominent of China's talent recruitment plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information.

According to Lewis's contract, the Chinese Academy of Sciences agreed to employ Lewis as a professor for at least three years. In return, Lewis agreed to maintain an active research program that yielded publications in high quality, peer-reviewed journals, and to provide research training and experience for Chinese Academy of Sciences students.

As a part of the program, Lewis was promised benefits, including a living subsidy of 1 million Yuan (approximately $143,000), a research subsidy of 4 million Yuan (approximately $573,000), and a salary of 600,000 Yuan (approximately $86,000). To receive the benefits, Lewis would have to work full time in China for three consecutive years, for no less than nine months per year, and would have to begin work no later than August 8, 2018.

In March 2018, Lewis submitted a request to WVU for an alternate/parental work assignment, requesting to be released from his teaching duties for the fall 2018 semester to serve as the primary caregiver for a child he and his wife were expecting in June 2018. In fact, however, Lewis knew this request was fraudulent. Rather than caring for his newborn child, Lewis planned to work in China during the fall 2018 semester as a part of his agreement with the "1000 Talents Plan." Based on the false justification Lewis offered, WVU granted his request.

In the fall of 2018, Lewis spent all but three weeks of the semester in China while his newborn child remained in the United States. During this period, Lewis received his full salary from WVU pursuant to his alternate/parental work assignment. Lewis's scheme allowed him to fraudulently obtain $20,189 from WVU.



CASE STUDY

Talent Poaching & Foreign Talent Recruitment

In December 2021, Dr. Charles Lieber, a pioneer in the field of nanoscience and the former Chair of Harvard University's Chemistry and Chemical Biology Department, was convicted by a federal jury of lying to federal authorities about his affiliation with China's Thousand Talents Program and the Wuhan University of Technology (WUT) in Wuhan, China, as well as failing to report income he received from WUT. In April 2023, Lieber was sentenced to time served (two days) in prison, two years of supervised release with six months of home confinement, a fine of $50,000, and $33,600 in restitution to the Internal Revenue Service.

Lieber had served as the Principal Investigator of the Lieber Research Group at Harvard University, which between 2008 and 2019 conducted more than $15 million in research sponsored by various U.S. Government agencies, including the U.S. Department of Defense (DOD) and the National Institutes of Health (NIH). Unbeknownst to his employer, Harvard University, Lieber became a "Strategic Scientist" at WUT and, later, a contractual participant in China's Thousand Talents Plan from at least 2012 through 2015. China's Thousand Talents Plan was one of the most prominent Chinese talent recruitment plans designed to attract, recruit and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity, and national security. The terms of Lieber's three-year Thousand Talents contract with WUT entitled Lieber to a salary of up to $50,000 per month, living expenses of up to $150,000 and approximately $1.5 million to conduct joint research at WUT.

In April 2025, after serving his sentence in the United States, Lieber took a full-time position as a faculty member at Tsinghua Shenzhen International Graduate School (SIGS) in China. SIGS also appointed Lieber as a chair professor, which is the university's highest faculty honor. The school's vice president, Wang Hongwei, said that Lieber's appointment "will significantly advance materials science and biomedical engineering development at Tsinghua University and Shenzhen, foster in-depth interdisciplinary collaborations between domestic and international research teams, and support the growth of young scholars into world-class scientists." The university's dean, Ouyang Zheng, stated that Lieber's participation at the university will "advance SIGS's academic excellence and contribute to the to the establishment of a world-class scholarly community."

CASE STUDY

Foreign Research Collaboration

- In December 2024, a U.S. university paid the Department of Justice a fine of more than $700,000 for failing to disclose that one of its researchers was being funded by a foreign government, while also seeking and receiving taxpayer research funds from NASA.
- In September 2024, another U.S. university paid more than $300,000 for failing to disclose that China was funding one of its scientists while the scientist also received funds from NASA and the National Oceanic and Atmospheric Administration.
- And in July 2024, another U.S. university paid a $500,000 fine over a similar set of issues. In this case, the principal investigator was being funded by Huawei Technologies Co., Ltd. while seeking a National Science Foundation taxpayer grant for research.

Foreign Research Collaboration

International research partnerships and collaborations are exploited in ways that allow foreign threat actors to acquire information to advance their own technology and innovation goals.

This trend is apparent in U.S. cases where principal investigators fail to disclose foreign government funding for research when applying for U.S. grants for the same or parallel research. In addition, principal investigators are generally not required to disclose lists of researchers that will work on the projects, who could nonetheless be collaborating on similar research with foreign universities without disclosing foreign government funding. The actual researchers that work under the principal investigator can have the same or similar access to the research. And just like the principal investigator, their foreign research collaboration can become a concern.

Providing false information on a grant application can lead to administrative and legal penalties.

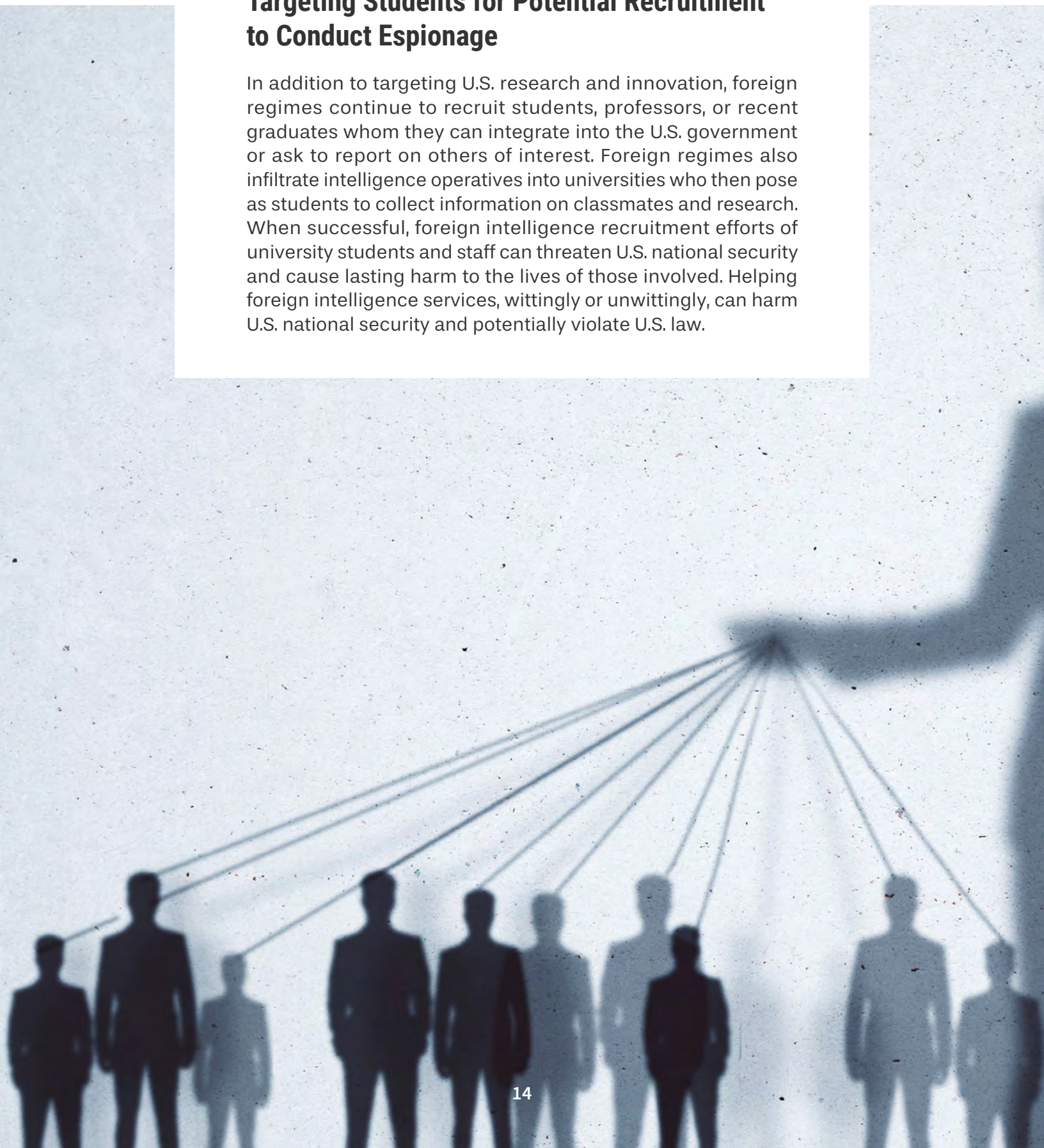
Collaboration is key for our research enterprise, but these omissions undermine the integrity of the research grant process. Professors, researchers, and students play an important role in protecting taxpayer-funded research, which is designed to benefit the American people, not foreign governments.

In 2023, a foreign national from a U.S.-sanctioned country emailed an academic professional (and cleared contractor) and requested collaboration on advanced missile technologies. The requested information would have provided hypersonic missile technology, considerably increasing military capabilities of the foreign national's country. Despite claiming expertise in an unrelated field, the foreign national claimed to have previously worked with U.S. academics on hypersonics.

"Non-disclosure of foreign collaborators" refers to the act of failing to reveal the involvement of researchers or institutions located outside of the U.S. when applying for funding or conducting research. In certain circumstances, failure to disclose foreign collaborations can lead to sanctions like loss of funding, revoked grants, and potential legal repercussions for the researcher and their institution. Transparency is crucial to address concerns about foreign influence on research, potential conflicts of interest, and ensuring proper oversight of research activities.

Targeting Students for Potential Recruitment to Conduct Espionage

In addition to targeting U.S. research and innovation, foreign regimes continue to recruit students, professors, or recent graduates whom they can integrate into the U.S. government or ask to report on others of interest. Foreign regimes also infiltrate intelligence operatives into universities who then pose as students to collect information on classmates and research. When successful, foreign intelligence recruitment efforts of university students and staff can threaten U.S. national security and cause lasting harm to the lives of those involved. Helping foreign intelligence services, wittingly or unwittingly, can harm U.S. national security and potentially violate U.S. law.



CASE STUDY

Recruitment for Espionage

- In April 2024, Victor Rocha was sentenced to 15 years in prison for serving as a Cuban agent for more than four decades. Rocha was recruited by Cuba after graduating from Yale and before graduate school. He then got a job at the State Department, later serving on the National Security Council and as U.S. Ambassador to Bolivia—all the while secretly operating as a Cuban agent.
- Ji Chaoqun, was a student in China who was recruited by China's Ministry of State Security (MSS) before he came to study in the U.S. While a student at a U.S. university, the MSS tasked Ji to collect information on U.S. aerospace engineers, including at defense contracting firms, for potential recruitment by the MSS. After graduating, he enlisted in the Army and was planning to get U.S. citizenship, then apply for a job at CIA or FBI. Before he could do so, Ji was arrested and sentenced to prison.
- From 2018–2020, Russia placed an intelligence operative posing as a Brazilian graduate student at Johns Hopkins University in D.C. From there, he could collect information on classmates, many of whom would go on to U.S. Government jobs. A few years earlier, Russia's intelligence service inserted an operative posing as a graduate student at Columbia University for the same purpose.

Impact

Although information sought by foreign adversaries may seem insignificant, the loss of such data can have negative and potentially costly impacts on researchers, academic institutions, and the U.S. innovation ecosystem.

Additionally, individuals and institutions who—wittingly or unwittingly—assist in the unauthorized transfer or theft of sensitive research or information, may face legal and financial consequences. This could include losing control over intellectual property, jeopardizing their professional credibility, and disqualifying them from future business or research opportunities, in addition to possible financial penalties and/or a jail sentence.

The impacts can also manifest themselves in a changing dynamic in the strategic power competition that has both national and economic security impacts for the U.S.—and ultimately inhibits our research and innovation ecosystem. For example, a May 2025 press report highlighted a nuclear breakthrough that would allow China to refuel a nuclear reactor without shutting down, taking China closer to limitless clean energy. This step positioned China to take the global lead in clean energy, largely driven by their ability to exploit publicly available U.S. research.

Indicators

Foreign adversaries use increasingly diverse methods to target and exploit U.S. research. Tactics include foreign talent recruitment programs, state-sponsored espionage, coercion of information from students and faculty, and technical/cyber techniques. Adversaries use them to lure intellectual property and talent away from U.S. universities and research centers, and to encourage unlawful behavior that puts scholars at risk. To help protect themselves and their work, researchers should learn to recognize the following potential indicators.

Elicitation

Elicitation is a subtle, structured method of collecting specific information from an unwitting target, disguised as a friendly, casual conversation.

- **Personal Contact:** The use of elicitation to collect information through seemingly routine contact. This can be used to confirm or expand knowledge of sensitive research, to gain clearer insight into a person's access, or to determine the potential to enlist the target for espionage or other collection and influence activities. Signs of this approach include: a professional contact requesting information outside the scope of a contract or a typical professional interaction; a request to shift communications outside official networks; or a casual acquaintance appearing to have unusual interest in, or knowledge of, your work.
- **Academic Solicitation:** The use of students, professors, scientists, or researchers to obtain sensitive or classified information. This can include a variety of unsolicited requests: for access to research papers/documents; for research applications; for academic peer reviews; to attend or present at an international conference; or to provide grants or gifting of funds/equipment from foreign academic institutions or governments.
- **Academic Consultation:** Academic scientists can be hired as consultants by real or fictitious companies with malign intent. The specialized knowledge of academic scientists can be leveraged by hiring them as short-term consultants who can provide expert insights into cutting-edge advancements, helping adversaries translate academic know-how into marketable technologies. This collaboration can accelerate product development, inform strategic research directions, and facilitate technology transfer by providing companies with access to specialized expertise and established research networks, effectively blurring the lines between academia and industry.

CASE STUDY

Elicitation

An American aerospace engineering professor at a university in Michigan accepted a Chinese student's request to study with him. The student expressed interest in the professor's research and indicated that she was affiliated with a Chinese civilian institution. However, it was later revealed that the student was in fact associated with a college for China's military officers. The professor admitted that the student pressured him to provide sensitive information about his work and seemed to want to use it for military satellite applications.

Insider Threats & Access

Any person with authorized access to sensitive information, research, or resources can become an insider threat if they use their position to harm their institution or organization. Trusted insiders—including students, faculty, and administrators—who are currently enrolled in or working at a U.S. university, can also be manipulated and coerced by foreign adversaries to illicitly obtain sensitive information and innovative research. Insider threats may display potential risk indicators, such as repeated security violations, failure to comply with overseas travel reporting requirements (where applicable), seeking to obtain information or research outside their security clearance or job scope, or allowing an unauthorized individual physical access to a research facility. Insiders are one of the greatest sources of intellectual property theft in the U.S. innovation enterprise.

Cyber Intrusions & Social Media

Foreign state adversaries also use cyber techniques to attack computers, manipulate codes or programming, and gain access to sensitive information —or to install invasive software—on a network. This can be done using a variety of cyber methods, such as click-baiting or phishing—to include leveraging email accounts from trusted domains or exploiting unpatched software. They may also collect intelligence utilizing publicly available information, exploiting social media, or through social engineering. Indicators include unsolicited and questionable contacts from unknown individuals on social media platforms, suspicious files sent via private message, requests for information, academic solicitation, or job offers from adversarial countries.

Cyber Intrusions & Social Media

- In March 2018, nine hackers working for the Mabna Institute (an Iranian government-sponsored entity) were indicted for allegedly conducting a massive cyber theft campaign which involved hacking into at least 144 U.S. universities and 176 universities in 21 foreign countries. The hackers allegedly stole 31.5 terabytes—about 15 billion pages—of academic data using a phishing campaign that successfully compromised 8,000 accounts to steal research and other academic data. Collectively, the victim universities spent an estimated $3.4 billion to reacquire the data.

- International expert network companies (ENCs) are part of a growing expert network industry whose intended purpose is to connect experts in various sectors to clients seeking non-publicly available information. In their most honest form, ENCs can help businesses use expert insights to gain a competitive edge and inform decision-making. However, in recent years, some ENCs have facilitated communication between unidentified third parties and U.S. cleared contractor employees, with the intention to gain and transfer protected information about defense technology to suspected foreign entities. In Fiscal Year 2023, ENCs sent requests to cleared contractors via email, social media messaging applications, and telephone calls, offering paid consultations to discuss sensitive technologies. This included hypersonic and missile technology, aeronautics systems, 5th generation fighter aircraft, space launch technology, Unmanned Aerial Vehicle (UAV) platforms, and cybersecurity. ENCs occasionally provided a list of questions for cleared contractor employees to answer, which would provide export-controlled or sensitive information related to U.S. defense platforms to those third parties. ENCs that contacted cleared contractor employees were based in China, Russia, the U.S., Hong Kong, the Philippines, the United Kingdom, Germany, Israel, and Canada, among others. ENC business models obscure the ultimate client, making them ideal for foreign intelligence entities and adversarial governments looking to gain sensitive information and technology from U.S. experts.

Jonathan Chadwick for MailOnline. "Nuclear breakthrough: China's experimental reactor refuels WITHOUT shutting down – taking the world closer towards limitless clean energy." 30 April 2025. The Daily Mail UK.

Mitigations

Institutions and individuals both have a responsibility to safeguard science. Security education can complement existing safety and ethics training by incorporating real-world case studies of research exploitation. Additionally, there are simple and proactive steps that can be taken to make informed decisions about potential risks on campus or when studying or traveling abroad, and to simultaneously strengthen confidence in international collaboration. Actions you can take are summarized in the table on the next pages.

Institutions

Secure Innovation

- Identify your vulnerabilities and risk tolerance and apply a risk-based approach to research security.
- Build and foster a strong security culture by creating an environment that enables, encourages, and educates faculty, administrators, staff, and students towards security-savvy behaviors.
- Establish a security governance model with sound and tested policies and procedures to support oversight, control, and decision-making.

Secure Your Research

- Protect the people, places, technology, and information that support your innovation (data, facilities, systems, devices, supply chains, etc.).
- Practices to consider include encrypting data at rest, enforcing multi-factor authentication (MFA) to systems/databases that house research, limiting remote logins, and blacklisting logins from foreign IP addresses.
- Segregate research and control access both physically and online. Consider enforcing policies like using designated equipment for all research (i.e., no storing sensitive research on personal devices, only transmitting research to/from academic accounts, ensuring emails are encrypted).
- Establish reporting procedures and educate faculty, administrators, staff, and students on indicators and reporting mechanisms.
- Use appropriate legal frameworks (contracts, grants, agreements, etc.) with explicit language. Consider export controls, legislation, and foreign investment.

Secure Your Partnerships

- Provide resources for faculty, administrators, staff, and students to conduct due diligence and consider conflicts of interest when assessing new research or funding collaborations.

Secure Your Success

- Manage security risks as you expand your footprint and portfolio.
- Comply with requirements to report sources of foreign funding
- Safeguard science – maintain trust, protect integrity, manage cumulative risk, mitigate financial loss, and protect your institution's reputation.

Individuals

- Actively participate in research security training and implement your institution's research security policies and procedures.
- Implement appropriate contractual agreements and administrative procedures while also complying with your institution's procedures for visas and visiting scientists.
- Practice good cybersecurity to reduce the likelihood of your research being lost or compromised.

- Throughout the research cycle, consider if there is anything patentable within your research, any risks of unauthorized transfer, or any dual-use applications.
- Ensure an appropriate segregation of information where necessary, to protect IP, research, or personal data—both physically and online.
- Work with your technology transfer office or its equivalent to determine if your research is subject to export controls or other legal or compliance requirements.
- Document and report security lapses and unauthorized behavior.

- Conduct due diligence on research partners and collaborators.
- When entering a new collaboration, including funding arrangements, understand the cybersecurity risks, and the security measures that reduce those risks.
- Follow appropriate procedures within your institution for visiting researchers and consider expectations you or sponsors may have regarding confidentiality and non-disclosure.

- Safeguard science – maintain your trust, integrity, and reputation by adhering to the policies, procedures, and values that protect the openness, collaborative nature and academic freedoms of the U.S. innovation ecosystem.

When traveling or studying overseas, including for academic and technical conferences, be security aware.

- ↳ Consider the country you are traveling to and be aware of local laws and customs.
- ↳ Consider how you will protect intellectual property and sensitive data.
- ↳ Think carefully about what information you share or present.
- ↳ Be clear about the areas of research you should or should not talk about.
- ↳ Be aware of who wants to establish further contact and cooperation.
- ↳ Reconsider carrying an electronic device with sensitive research data on the hard drive
- ↳ Do not leave electronic devices unattended.
- ↳ Practice good cyber hygiene. Sanitize your laptop and mobile phone prior to travel and ensure no sensitive contact, research, or personal data is on them. Enable device decryption on all devices. If feasible, use a different phone and email account while traveling. Use up-to-date protections for antivirus, spyware, security patches, and firewalls.

Additional Resources

The previous recommendations are important first steps. The following resources provide additional guidance and best practices to manage risks and prevent harm to U.S. economic and national security:

- **National Counterintelligence and Security Center (NCSC)**: Secure Innovation (www.dni.gov/index.php/ncsc-what-we-do/secure-innovation)
- **National Science Foundation (NSF)**: Research security resources (www.nsf.gov/research-security)
- **National Institute of Standards and Technology (NIST)**: Safeguarding International Science Research Security Framework and other research security resources (www.nist.gov/adlp/research-security-office)
- **Defense Counterintelligence & Security Agency (DCSA):** DCSA's Center for Development of Security Excellence (CDSE) provides security education, training, and certifications for the DOD and industry under the National Industrial Security Program (www.cdse.edu)
- **SECURE Center**: The SECURE Center, standing for **S**afeguarding the **E**ntire **C**ommunity of the **U**.S. **R**esearch **E**cosystem, is a non-government, independent entity formed to address foreign government interference, support security-informed decision-making, and serve as a conduit that connects research community stakeholders with one another and with U.S. government (USG) agencies via NSF (secure-center.org)
- **SECURE Analytics**: NSF SECURE Analytics is the data collection, analysis and reporting hub for the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Program, established by the U.S. National Science Foundation (NSF), to train and enhance the research community's ability to mitigate and prevent foreign interference in research (secure-analytics.org)

For additional information on NCSC threat awareness materials or publications:

Visit www.ncsc.gov

Contact NCSC_Outreach@odni.gov

Follow NCSC for more information

Lorem ipsum

Reporting

You are the first line of defense to protect your research by reporting suspicious activity, behaviors, indicators, concerns, or vulnerabilities. Report suspicious efforts to gain access to information, via the links below.

- Contact your campus police, research security office, or other appropriate professor, instructor, or administrator.
- Engage with your local FBI Field Office. Report suspicious activities or outreach by foreign-linked actors to your local FBI field office at www.fbi.gov/contact-us/field-offices. You can also contact tips.fbi.gov or call 1-800-CALL-FBI.
- Cleared academic institutions are required to report suspicious contacts, behaviors, and activities in accordance with Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM). If you suspect you or your academic institution has been targeted, report it immediately to your local DCSA counterintelligence agent.
- To report a computer security incident, the Internet Crime Complaint Center (IC3) is the central hub run by the FBI for reporting cyber-enabled crime: complaint.ic3.gov.

For additional information on NCSC threat awareness materials or publications:

Visit www.ncsc.gov

Contact NCSC_Outreach@odni.gov

Follow NCSC for more information

August 2025