SAFEGUARDING ACADEMIA

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

Quick Reference Guide for Students and Researchers

Academic freedom, open collaboration, and the exchange of ideas are essential for scientific progress and innovation. However, these same values are being exploited by foreign threat actors seeking to advance their own strategic and technological objectives, which are often at odds with core U.S. interests. These actors use techniques such as unauthorized access, illicit data transfer, and covert recruitment to target U.S. research, often without the knowledge or consent of U.S. institutions. You can take proactive measures to help ensure your and your institution's intellectual property and research integrity remain protected while preserving the values that foster academic advancement.

Who Targets Academia?

- Foreign intelligence entities
- Foreign research organizations
- Competitors and state-backed companies
- Disgruntled and opportunistic insiders

Common Indicators of Threats

- Unauthorized requests to access sensitive or U.S. government-funded research
- Sudden unexplained affluence of researchers, administrators, faculty, staff, or students
- Working odd hours or undisclosed foreign travel to facilitate the unauthorized transfer of intellectual property
- Solicitation by foreign recruitment programs offering unusually lucrative incentives
- Unsolicited contacts, especially from foreign entities via social media or academic platforms
- Guidance to obscure or not report contact or affiliation with a foreign entity

Recent Cases

- *Advanced Materials Recruitment*: A Chinese government-backed center offered substantial research funding and incentives to a U.S. researcher for sensitive information.
- *Undisclosed Foreign Funding*: Multiple U.S. universities were recently fined for failing to disclose researchers who had received NASA and NSF funding had affiliations with China.

Protecting Your Innovation

- **Secure Your Environment:** Receive security training; follow institutional protocols on foreign collaborators, institutions, and visitors.
- **Secure Your Research:** Identify potential dual-use (civilian/military) projects; segregate sensitive data; take extra steps to protect U.S. government-funded research; consult tech transfer offices on export regulations.
- **Secure Your Partnerships:** Vet collaborators and funding sources; maintain strong cybersecurity; uphold confidentiality agreements.
- **Secure Your Success & Safeguard Science:** Know foreign country local laws and risks; secure data during travel; avoid oversharing at conferences.
- **Report** foreign threat actors targeting your research to the FBI at 1-800-CALL-FBI, tips.fbi.gov, or your local FBI field office: www.fbi.gov/contact-us/field-offices. If your research is in support of a cleared academic institution and you suspect you or your academic institution has been targeted, report it immediately to your local DCSA counterintelligence agent.

By fostering an environment of security awareness, researchers can protect their intellectual property and ensure the integrity of their work. Proactive measures and a vigilant approach can help safeguard your valuable research, allowing academic communities to collaborate with confidence.

To learn more about what you can do to protect your research and safeguard science, see the bulletin "Safeguarding Academia" at www.ncsc.gov.

For additional information on NCSC threat awareness materials or publications:

Visit www.ncsc.gov   Contact NCSC_Outreach@odni.gov   Follow NCSC: