SAFEGUARDING ACADEMIA

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

Quick Reference Guide for Academic Institutions

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. Institutions that—wittingly or unwittingly—assist in the unauthorized transfer or theft of sensitive research or information may face reputational and financial consequences including losing control over research and data, losing future research opportunities, and paying substantial fines. Your role as a research administrator is essential in guiding informed decisions about potential risks and taking proactive measures to safeguard research, 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

These activities might seem helpful or harmless, but adversaries can use them to steal research and talent and push scholars into risky or illegal situations that may harm the institution.

- Invitation to a foreign program offering unusually lucrative incentives or requesting no formal written agreement
- Unsolicited grants or gift funding from foreign institutions
- Unsolicited offers of research positions or paid international conference engagements
- Requests for research access or engagement through social media

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 Institution

- **Secure Your Environment:** Assess risks and apply a security strategy. Establish governance with cross-functional oversight and a strong security culture at all levels of the institution.
- **Secure Your Research:** Use institutional templates and reviews for research agreements. Protect data and implement access controls. Ensure compliance with export controls, disclosure requirements, and funding rules.
- **Secure Your Partnerships:** Conduct vetting of collaborators, sponsors, and funding sources.
- **Secure Your Success & Safeguard Science:** Promote a culture of safeguarding federal investments through training and awareness.
- **Report** foreign threat actors targeting your institution to the FBI at 1-800-CALL-FBI, tips.fbi.gov, or your local FBI field office: www.fbi.gov/contactus/field-offices. If you are 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, institutions help protect the U.S. research ecosystem. Proactive measures and a vigilant approach yields a safe and empowered scientific community and enable researchers to collaborate without worrying their valuable work will be stolen or misused.

To learn more about what you can do to protect your institution 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: