Updates
August 09, 2023
New Risk-Based Security Requirements for Federally Funded Research at US Institutions of Higher Education

International cooperation and welcoming foreign academics are critical to the success and leadership of U.S. institutions of higher education.

These interactions enhance fundamental scientific research and promote the American tradition of attracting scientific, technical, and cultural talent from around the world.

The U.S. government supports international academic collaboration, but has struggled in recent years to identify and respond to some foreign governments' exploitation of U.S. academic openness to exert influence or acquire research information. These results may be the foreign government's goal, or they may be unintended consequences of incomplete transparency. In either case, they present risks ranging from inefficient funding decisions and depriving U.S. institutions of the fruits of their research to providing an avenue for foreign governments to operate in the United States through undeclared agents.

The federal government continues to refine its approach to these risks while encouraging international academic engagement and avoiding the appearance of unfair targeting of particular nationalities or ethnicities. In 2021, the White House released the National Security Presidential Memorandum-33 (NSPM-33), which directed federal agencies to standardize and enhance disclosure and security requirements that apply to federally funded research and development. According to NSPM-33, the government's goal is to "foster research discoveries and innovation" while also taking "steps to protect intellectual capital, discourage research misappropriation, and ensure responsible management of United States taxpayer dollars." For more information on NSPM-33, please see here.

Recent guidance from the U.S. Department of Defense (DoD) expands on the directives in NSPM-33. In June 2023, the Office of the Undersecretary of Defense for Research and Engineering (OUSD R&E) released a new policy memorandum that requires all research projects funded by DoD to go through risk-based security reviews. These reviews are intended to: (1) ensure security of DoD-funded research; (2) require disclosure of information

that may reveal potential conflicts of interest and commitment; and (3) provide clear messaging regarding the activities that may create challenges in receiving DoD research funding, including, but not limited to, relationships with foreign recruitment programs or funding from a country of concern (such as the People's Republic of China [PRC], the Russian Federation, and Democratic People's Republic of Korea [DPRK]). This policy addresses some of the unanswered questions that remained after prior implementation and enforcement efforts, such as consistency in how standards are applied and the significance of specific types of foreign commitments, awards, and appointments.

The new policy requires DoD funding components to adopt risk-based security review processes to determine whether proposals selected for awards require risk mitigation. The policy takes steps to standardize the funding components' reporting requirements and refers to a publicly available decision matrix that DoD components will apply to mitigation decisions. DoD further directs components to implement these processes in a manner that does not discourage international collaboration and that does not unduly prolong time to award.

DoD's announced policy provides U.S. research institutions with a framework for proactively assessing both disclosure requirements and security risks associated with investigators' support from and commitments to foreign governments. It also lists potential mitigation strategies such as insider risk training, additional reporting requirements, staffing changes, review of foreign contracts, and requiring an investigator to terminate a foreign obligation.

U.S. research institutions can use the DoD policy to anticipate and address research security issues through their management of the award application and research integrity processes. Recommendations include:

1. **Developing and implementing appropriate policies, procedures, and processes to identify, address, and mitigate risks associated with research funded by a foreign government. Such policies should include formal processes and voluntary procedures.** Examples of policies include relevant sections on research funded by foreign governments in university handbooks and manuals, established security review procedures as described above, and ensuring full managerial control over any research program funded by a foreign government.
2. **Promoting a culture that furthers the core values of U.S. higher education.** As explained by OUSD R&E, "[i]nternational collaboration is an important mechanism for ... promoting progress in fundamental research." Despite the need for risk-based security measures, U.S. institutions of higher education should continue to promote an environment encouraging academic freedom, innovation, and research.
3. **Considering whether the partnering nation is a country of concern.** The OUSD R&E policy memorandum includes a list of research institutions in China, Russia, North Korea, and Iran that "have been confirmed as engaging in problematic activity." If a U.S. institution of higher education insists on partnering with any of these institutions, there should be additional vetting procedures to better understand the additional risks.
4. **Bolstering the dissemination of information to administrators, faculty, and staff regarding the process used to review and initiate foreign-funded collaborations.** Communication is a key step in ensuring compliance with relevant procedures.

U.S. institutions of higher education must strategically and proactively implement these practices to ensure compliance with required mandates and shield themselves against the risks associated with research funded by foreign governments. For more information about developing individualized practices for a university, please contact experienced counsel.

Authors

Explore more in

Government Contracts Private Client Services Data Security Counseling and Breach Response

Related insights

Update

Forthcoming Disclosure and Security Requirements for Institutions Hosting Federally Funded Research