The U.S. Government Accountability Office (GAO) thinks the FBI and other agencies are not doing enough to address the espionage threat on U.S. university campuses. It issued a report, “Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities” on June 14, 2022, urging the FBI, the Department of Homeland Security, and the Department of Commerce to step up their outreach efforts to address the threat. Commerce, DHS, and FBI have all concurred with GAO’s recommendations. As a result, U.S. colleges and universities to face yet another organizational risk: an increase in campuses visits by export control and law enforcement agents.

The threat: U.S. export control laws consider the disclosure to non-U.S. persons of technology, software, or technical data to be exports, even if the disclosure occurs in the United States.
The overwhelming majority of non-U.S. persons studying and working at U.S. universities are not security risks and are valued members of their academic organizations. But U.S. intelligence agencies have long warned that foreign state actors actively acquire sensitive national security data and proprietary technology from U.S. universities.

A lot of the technology flow abroad from U.S. universities is perfectly legal, for two reasons: First, most university research, even in cutting-edge technology, is exempt from export controls under an exemption known as “fundamental research.” Second, even in cases where the fundamental research exemption does not apply, it takes time for the U.S. government agencies to add new items to the export control lists they enforce; namely the U.S. Munitions List, administered by the U.S. Department of State, Directorate of Defense Trade Controls; and the Commerce Control List, administered by the U.S. Department of Commerce, Bureau of Industry and Security.

But at the same time, either through inadvertence or outright espionage, unlawful transfers of technology to foreign nationals take place. A 2006 report by the U.S. Office of the National Counterintelligence Executive found that a significant quantity of export controlled U.S. technology is released to foreign nationals in the United States unlawfully each year.

**Clash of values:** One important issue for higher education in addressing trade controls compliance is cultural in nature. U.S. universities value open, collaborative environments which drive and accelerate innovation. For those institutions, the idea of cutting off information flows conflicts with those cultural norms. By contrast, U.S. export controls aim to protect U.S. national security by hindering the flow of sensitive information to potential adversaries.

**GAO’s recommendations:** The GAO report recommends that U.S. trade control agencies take more aggressive steps to curb foreign access to sensitive technologies at U.S. universities. The recommendations include steps to enhance risk assessment and ranking of universities by risk, and steps to increase agency cooperation in planning and conducting outreach visits to universities. As a direct result of this report, U.S. universities are going to receive more visits from U.S. government agents.

**Practical takeaways:**

- **Universities:** Consider reevaluating your risk. The threat has evolved, and the U.S. government response is also evolving. A risk evaluation using modern tools such as a premortem can help you know where to dedicate resources to update your export control policies, procedures, and training. Any unlawful escape of technology or technical data are much more likely to be detected and punished under the new regime, in part based on the GAO report. Organizations have to evolve with the threat.

- **Students, faculty, and administrators:** Consider how to jealously guard your academic freedom, but be wary of the national security risks of sensitive technology falling into the wrong hands.

- **Research sponsors:** More and more U.S. university research is sponsored by U.S.
companies and government agencies. Research sponsorship agreements play a major role in striving for both national security and academic goals of the U.S. university system. Sponsors need to be sensitive to how these agreements are drafted. Sponsors must be aware of the espionage threat to their technology. But imposing too many restrictions in the contract may undermine the applicability of the fundamental research exemption and hinder the success of the project.

**Conclusion:** In the face of organizational threats, institutions do best when they heed their values. In the realm of protecting sensitive technology, we must constantly evolve with the threat. But we must also continue to carefully balance national security considerations with our bedrock values of academic freedom and openness.

Copyright © 2022, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume XII, Number 223