JUNE 2026

COMPLIANCE & ETHICS PROFESSIONAL

CEP MAGAZINE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

BAILEY MACK, CCEP, CHPC
CHIEF COMPLIANCE OFFICER AT TOGETHER FOR YOUTH AND THE HOUSE OF THE GOOD SHEPHERD

COMPLIANCE IS INFRASTRUCTURE, NOT CONSTRAINT (P6)

SCCE®

UNIVERSITIES IN THE CROSSHAIRS: NAVIGATING FOREIGN ESPIONAGE AND RESEARCH SECURITY RISKS

by T. Markus Funk and Brent Wible

CCB article click for CEU quiz

T. Markus Funk

(mfunk@whitecase.com) is a Band 1 White & Case Partner, former federal prosecutor, and conflict-deployed State Department Section Chief.

Brent Wible

(brent.wible@whitecase.com) is a Partner at White & Case and a seasoned former federal prosecutor with extensive experience handling sensitive investigations, including ones that implicate national security concerns.

Universities increasingly find themselves the direct target of U.S. national security enforcement, as federal scrutiny expands beyond grant disclosures to allegations of espionage and intellectual property (IP) theft on campus. And all indications are that even more ramped-up governmental attention is on the horizon.

These matters are far removed from routine compliance issues. They unfold quickly, often quietly, and can place federal funding, institutional reputation, and academic mission at immediate risk.

Drawing on recent U.S. Department of Justice (DOJ) and state enforcement trends, this article explains why early reactions matter, how common missteps amplify exposure, and what institutions should do in the critical first days of government attention. It also outlines concrete, defensible strategies for strengthening research security and governance without sacrificing academic freedom or inviting discrimination claims. The result is a practical guide for higher-education leaders navigating one of the most consequential risk landscapes facing universities today.

Academic institutions facing government investigations

In recent years, DOJ has brought enforcement actions under the False Claims Act (FCA) against multiple universities for failing to disclose, in federal grant applications, their researchers' ties to foreign governments and foreign research support. These resolutions typically involved grants from the U.S. Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA), given their national security nexus and restrictions on foreign affiliations.

DOJ's focus on sensitive research at academic institutions may now be expanding from disclosures about researchers' foreign affiliations to allegations of espionage or IP theft on campus. As the U.S. government's focus shifts, universities should prepare for increased investigative scrutiny and an escalation of enforcement activity.

A national security problem lands on campus

If the U.S. government concludes that a foreign student or faculty or staff member has engaged in espionage or IP theft, the university or research institution will confront a

challenge fundamentally different from ordinary compliance or employment matters.[1] These cases sit at the intersection of national security, immigration law, federal research funding, civil rights, both civil and criminal enforcement, and academic freedom. Put another way, this is a juncture where missteps are particularly easy, and forgiveness is rare.

Unlike familiar regulatory inquiries, national security-related investigations tend to unfold quickly, often behind closed doors, and with consequences that can extend far beyond the individual under scrutiny. Federal funding decisions, congressional attention, donor confidence, and institutional reputation can all hang in the balance.

In that environment, how a university or affiliated research institution responds in the first days and weeks will shape not only the government's approach, but also the institution's standing with its own faculty, students, funders, and the public.

Slowing down the initial response

When allegations first surface, whether through law enforcement outreach, a funding agency inquiry, media mention, or internal reporting, the most important early decision is what *not* to do. More specifically, experience teaches that universities should resist the urge to issue immediate public statements, quickly terminate affiliations, or take speedy immigration-related action. Although acting in a time-sensitive manner is crucial, it is even more critical that they first understand the basic nature and scope of the concerns.

What is needed is a controlled, thoughtful internal assessment. A small response team, led by the general counsel's office and supported by experienced outside counsel where appropriate, should immediately take charge. Document preservation is essential. Research data, access logs, grant materials, lab notebooks, and communications with sponsors must be preserved before routine deletion or system updates complicate matters.

At this stage, institutions should focus on access and controls rather than motives. Who had access to which systems, data, or facilities? Under what restrictions? Were those restrictions followed? These questions — not speculation about intent or geopolitics — will drive the government's analysis and ultimately determine the institution's legal and reputational exposure.

The value of being proactive before trouble starts

Universities that have invested in research security before a crisis, including digital and physical security, strict access controls, security training, and vetting visiting scholars, post-doctoral students, and lab personnel — among other steps — will find themselves in a much stronger position. Federal agencies have been explicit in recent years that institutions are expected to understand where their most sensitive research resides and how it is protected.

For example, in January 2021, the Biden administration issued National Security Presidential Memorandum-33 (NSPM-33), implemented through the Office of Science and Technology Policy.[2] NSPM-33 squarely places responsibility on research institutions to identify, track, and safeguard sensitive research and data. And far from mere aspirational language, NSPM-33 ties federal funding eligibility to an institution's ability to map and protect sensitive research assets, making awareness and protection an affirmative institutional obligation.

Further, the National Institutes of Health (NIH), under Trump-appointed leadership, in July 2025 issued new mandatory policy requirements for institutions receiving federal funding that clearly tie institutional understanding and oversight of research activities to eligibility for funding.[3] Rather than leaving research security implicit, NIH now mandates training and institutional certification tied to federal awards. It requires institutions to know (and document that they know) the sources, scope, and risks associated with their research portfolios. That creates accountability precisely in the areas of sensitive support disclosure and research oversight.

As touched on earlier, DOJ has shifted its enforcement strategy regarding undisclosed foreign affiliations, largely Chinese, in academic research. It has moved from criminal prosecutions of individual researchers under the now-defunct "China Initiative" to civil enforcement actions against academic institutions using the FCA. Since ending the China Initiative in 2022, DOJ has targeted universities for failing to disclose researchers' Chinese ties on federal grant applications, resulting in several high-profile FCA settlements with institutions such as Stanford and the University of Maryland.[4] This approach allows DOJ to pursue treble damages under a lower burden of proof than criminal cases. Recent investigations have particularly focused on grants from agencies like NASA and DoD,

where regulatory restrictions on foreign affiliations are particularly stringent.

Now more than ever, expectations that universities will not only fully disclose foreign affiliations but also implement controls to safeguard sensitive IP permeate virtually all aspects of higher education and research. Advanced computing, AI, biotechnology, quantum research, and proprietary industry partnerships all attract scrutiny. Meaningful conflict-of-interest disclosures, audits of foreign affiliations, access controls tied to risk rather than rank, and faculty training on deemed exports are no longer aspirational best practices; they are increasingly treated as baseline obligations.

In response to this heightened scrutiny, academic institutions are wise to proactively mitigate risk by implementing comprehensive compliance measures. These include implementing digital and physical security and strict access controls, testing the effectiveness of those controls, educating faculty and staff on both security and disclosure requirements, adopting clear guidelines on foreign affiliations, requiring full disclosure of foreign gifts and employment and conducting due diligence to identify potential or suspected foreign ties, vetting visiting scholars, coordinating compliance efforts across departments, standardizing grant processes, auditing submissions, correcting any discrepancies, and engaging with peer institutions to stay informed of best practices. Failure to take these proactive steps may expose institutions to significant legal and financial liability, as DOJ expects universities to actively investigate and address potential foreign influence in federally funded research.

Additionally, emerging best practices instruct that these measures must not only be demonstrably effective but also content-neutral. Risk-based controls focused on the nature of the research are far more defensible than reactive approaches tied to citizenship or nationality, which invite discrimination claims and public backlash.

Managing the relationship with federal investigators

When federal authorities become involved, often through the Federal Bureau of Investigation or DOJ prosecutors, universities must strike a careful balance between cooperation and institutional self-protection.

Cooperation is, of course, expected, but it should also be disciplined, thoughtful, and protective of the institution's interests. Communications should be centralized through counsel. The institution should seek clarity on the scope and legal basis of requests, develop a positive, trust-based rapport with the specific regulators or enforcers, and ensure that document productions are not only accurate but also contextualized. Informal interviews or ad hoc disclosures by faculty members — once an investigation is apparent — can create inconsistencies that threaten to significantly complicate later stages of the inquiry.

At the same time, cooperation does not require surrender. Privileged material should remain protected, and student privacy obligations must be respected. Universities are not law enforcement agencies. Attempts to swiftly prop up quasi-criminal internal investigations — particularly if run by lawyers with no white-collar defense and investigations experience — often create more long-term problems than they solve.

State enforcement and regulatory risk

Although federal authorities currently drive most high-profile investigations, state-level action is increasingly relevant and, in some jurisdictions, imminent. State attorneys general have begun invoking consumer protection statutes, state FCAs, and nonprofit oversight authority to scrutinize universities' disclosures, governance, and handling of foreign funding and research partnerships, particularly at public or state-funded institutions. Several states have also enacted or proposed laws restricting foreign gifts, employment, or research collaborations in sensitive fields, creating parallel compliance regimes that may diverge from federal standards. As federal enforcement accelerates, coordinated or follow-on state investigations — often shaped by local political pressures — represent a growing, and often underappreciated, source of legal and reputational risk for universities.

Enrollment, employment, and immigration decisions

Decisions affecting a student's enrollment, employment, or visa sponsorship are among the most sensitive an institution can make. These actions can have immediate and irreversible consequences and are often scrutinized long after the investigation concludes.

Universities should ensure that any such steps are grounded

in documented policy violations or demonstrable security risks, rather than generalized suspicion or external pressures. Actions that appear rash or tied to nationality or country of origin are particularly vulnerable, especially where the government's own investigation remains unresolved.

Careful documentation of decision-making is essential, as these cases frequently resurface in civil litigation, administrative reviews, or congressional inquiries.

Public messaging without making things worse

Public communications is an area where institutions often stumble. Silence can look evasive; overreaction can look political or discriminatory. The most effective messaging emphasizes process rather than conclusions: cooperation with authorities, commitment to research integrity, and respect for the rule of law.

Equally important is reassurance. Universities must communicate clearly to international students and faculty that lawful study and research remain welcome and valued. Failure to do so can chill collaboration far beyond the individual case, undermining the institution's academic mission.

Board oversight and long-term institutional risk

Behind the scenes, boards of trustees should remain carefully briefed and closely engaged. National security investigations, for example, can affect federal funding streams, strategic partnerships, and long-term research priorities. Trustees, even before issues emerge, should be asking whether compliance resources align with research ambitions and risk exposure, and whether governance structures are equipped to manage sustained scrutiny.

A deliberate path forward

Allegations that foreign students or faculty are spying or stealing U.S. IP place universities in an unenviable position. Institutions that respond methodically by remaining carefully focused on facts, grounded in law, and disciplined in messaging, are best positioned to protect both their legal footing and their academic mission. Those who react hastily or impulsively may find that the collateral consequences far outlast the investigation itself.

Endnotes

1. Wil Courtney and Virginia Black, "Purdue complies with request for information on Chinese students," *Journal & Courier,* April 4, 2025, https://www.jconline.com/story/news/local/purdue/2025/04/04/purdue-complies-with-request-for-information-on-chinese-students/828.837.11007/.
2. Joseph R. Biden, "Presidential Memorandum on United States GovernmentSupported Research and Development National Security Policy," January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.
3. National Institutes of Health, "Notices of NIH Policy Changes," accessed April 7, 2026, https://grants.nih.gov/policy-and-compliance/notice-of-policy-changes.
4. U.S. Department of Justice, Office of Public Affairs, "Stanford University Agrees to Pay $1.9 Million to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals," news release, October 2, 2023, https://www.justice.gov/archives/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign; U.S. Department of Justice, U.S. Attorney's Office for the District of Maryland, "University of Maryland, College Park Agrees to Pay $500,000 to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals," news release, July 16, 2024, https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed.

Takeaways

- U.S. Department of Justice (DOJ) scrutiny of universities is expanding from grant disclosure issues to potential espionage and intellectual property theft risks.
- Early missteps (public statements, quick terminations, or immigration actions) can significantly increase legal and reputational exposure.
- Strong research-security programs, including access controls and training, position universities better when investigations arise.
- DOJ increasingly uses civil False Claims Act actions against universities for undisclosed foreign affiliations, leading to high-profile settlements.
- Effective responses require disciplined cooperation with investigators, content-neutral controls, and careful messaging to avoid discrimination or reputational damage.