LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Expect National Security Scrutiny Of Higher Ed To Continue

By **Michael Atkinson, Caroline Brown and Jeremy Iloulian** (January 9, 2024, 4:30 PM EST)


Michael Atkinson


Caroline Brown


Jeremy Iloulian

2023 was a significant year for U.S. universities and research laboratories, as their responsibilities to implement newly enacted U.S. requirements increased, and they came under greater federal government scrutiny, both in an effort to protect U.S. national security.

As has been the case for several years, 2023 showed that threats to U.S. national security arise from competition over advanced technologies. These technologies, which include artificial intelligence, quantum computing and semiconductors, will determine future military and economic supremacy.

Moreover, this competition has manifested itself in fights over capital investments in advanced technologies, efforts to secure — or, conversely, steal — the underlying intellectual property, and concerted actions to ensure access to the technologies and their critical raw materials, especially data, rare earth metals, and human talent.

In recognition of these threats, the U.S. government enhanced its national security enforcement capabilities, imposed new investment and technology transfer requirements, and began to implement these measures with the goal of countering technological advancement and influence from so-called countries of concern, principally China, Russia, Iran and North Korea, as well as U.S. export-restricted and sanctioned persons.

While these measures affected many U.S. economic sectors and institutions, one set of institutions has felt the effects the most and will continue to feel them in the coming years: U.S. universities and research laboratories.

Collectively, these measures have significantly elevated the national security responsibilities that academic communities now have. This, in turn, has elevated their legal and reputational risks.

As part of its attempts to limit foreign influence in the area of research security, in particular, the U.S. government has expressed increasing concern about foreign talent programs, and other associations and affiliations to countries of concern or U.S. export restricted and sanctioned persons.

We anticipate these trends will continue in 2024, with increasing scrutiny on academic communities and

researchers that intersect with national security; new controls on investments and talent pools for technology areas — where China, in particular, appears close to securing strategic advantages; and more regulatory, civil fraud and criminal law enforcement actions, and congressional scrutiny.

Universities and laboratories should enhance their compliance programs to stay in step with regulatory requirements and consider implementing additional safeguards to mitigate reputational risks.

Institutions should continuously evaluate their risk profile as risks increase and the U.S. government enacts additional compliance standards, adjusting their compliance programs accordingly by engaging in internal audits of compliance processes and internal reviews of any identified potential violations of these policies.

2023 Developments Related to Research Risk and Compliance

Executive Branch: Interagency Cooperation and Prioritization

In February 2023, the U.S. Department of Commerce's Bureau of Industry and Security and the U.S. Department of Justice announced the creation of the Disruptive Technology Strike Force.[1] The strike force brought together experts from the Federal Bureau of Investigation, Homeland Security Investigations and 14 U.S. attorneys' offices to target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries, specifically China, Russia, Iran and North Korea.[2]

Five cases brought by the DOJ against a series of individuals in May, August, September, November and December have been the most visible results of the strike force's actions.[3]

In July 2023, the BIS, the DOJ and the U.S. Department of the Treasury's Office of Foreign Assets Control issued the second tri-seal compliance note,[4] outlining each agency's respective voluntary self-disclosure procedures for potential violations of U.S. export controls and sanctions.[5] This compliance note encouraged private sector actors to make such disclosures, and emphasized their mitigating effects against potential penalties — at times up to a 50% reduction in penalties or no penalty issued at all.[6]

These cooperative efforts between the DOJ, the BIS, OFAC and other agencies are part of an ongoing trend in which the DOJ is prioritizing enforcement of national security laws, especially export controls and sanctions. In September 2023, for example, the DOJ's National Security Division hired its first-ever chief counsel and deputy chief counsel for corporate enforcement, after previously committing to hiring 25 new prosecutors.[7]

The DOJ also announced a settlement with Stanford University in which Stanford agreed to pay $1.9 million to settle allegations that it knowingly failed to disclose current and pending financial support of 12 faculty members in 16 different research grant proposals, in violation of the False Claims Act. The DOJ led this effort on behalf of the U.S. departments of the Army, Navy and Air Force, NASA and the National Science Foundation.[8]

The DOJ was not the only agency actively pursuing new actions to mitigate U.S. national security risks emanating from fundamental research or technological theft. In February 2023, the White House Office of Science and Technology Policy published draft standards for research security programs requirements,[9] as mandated by National Security Presidential Memorandum 33.[10]

Among those topics addressed in the OSTP draft standards were the parameters for compliance and training programs, the necessary security for foreign travel and cybersecurity.

In order to implement the requirements set out in NSPM-33, in June 2023 the U.S. Department of Defense issued a memorandum directed toward those research facilities that receive DOD funding, setting forth new requirements to counter unwanted foreign influence, including processes for the DOD's consideration of research proposals from higher education institutions.[11]

The DOD memorandum focused on security threats posed by China, Russia, Iran and North Korea, persons on the U.S. export controls and sanctions lists, and foreign talent programs in order to identify protocols that universities must establish to mitigate those risks.[12]

Congressional Action: Investigations

After the new U.S. House of Representatives took office last year, the House leadership set up a new select committee, the U.S. House of Representatives Select Committee on the Chinese Communist Party, which has all of Congress' investigatory powers — although it is unable to draft legislation. The select committee has been an active investigator, sending letters to corporations, nonprofits and other entities, including prominent universities, regarding potential violations of U.S. law and affiliations with China.

In June, the select committee wrote to Alfred University, expressing concern that Alfred University was both hosting a Confucius Institute — a Chinese cultural center that has been accused of being an outpost for Chinese Communist Party propaganda — and had also received $13.5 million in funding from the DOD, in violation of U.S. law.[13] Within the month, Alfred University shut down the Confucius Institute.[14]

Following the positive response from Alfred University, in July the select committee sent a letter to the University of California, Berkley, requesting information about UC Berkley's joint institute with Tsinghua University and the Shenzhen government in China — the Tsinghua-Berkley Shenzhen Institute.[15]

The letter cited research security risks presented by indirect ties with persons on the BIS Entity List as well as potential violations of Section 117 of the Higher Education Act, which requires institutions of higher education that receive federal financial assistance to disclose gifts received from, and contracts with, a foreign source that, alone or in combination, are valued at $250,000 or more in a calendar year.

Though no financial penalties have been exacted, the issuance of the letter highlights the reputational risks that universities and laboratories face.

Restrictions and Enforcement Actions Expected in 2024

Executive Branch Action: More Regulations and Enforcement

Additional U.S. government agencies may promulgate compliance requirements as a condition of receiving research funding, similar to those included in the DOD's June 2023 memorandum implementing NSPM-33.

For example, a matrix included in the DOD memorandum, which identifies the potential national security risks for which the DOD is looking and how the DOD will evaluate those risks, previews what

may come from other agencies.

The DOD explains that risks can develop if there exist any affiliations or associations between (1) any of the universities receiving funding or the individuals participating in research, and (2) any countries of concern, U.S. export controlled or sanctioned persons, or foreign talent programs. The DOD noted that the connection could be as limited as co-authoring articles with persons engaged in research at Chinese or Russian universities designated on U.S. export restricted or sanctioned persons lists.

Next, as evidenced by the strike force and the July 2023 tri-seal compliance note, agencies are collaborating with each other more frequently in an effort to leverage resources to identify potential violations where enforcement or heightened scrutiny may be appropriate.

While most institutions seem to be generally aware of existing deemed export risk, such as, for example, the provision of export-controlled technology or software to a non-U.S. person within the U.S., those same institutions rely on the U.S. export control exemption for fundamental research — e.g., the technology is not subject to U.S. export controls and thus there is no deemed export.

Yet, many of the new rules do not allow for a fundamental research exemption, even if the U.S. export controls do, a trend we expect to continue. A single technical violation, even an inadvertent violation, may provide U.S. government agencies with an opportunity to expand any review.

Congressional Action: Legislation and More Investigations

Universities are now a ripe target for the Republican-led House of Representatives and are likely to be in the crosshairs of any China-related legislation. The National Defense Authorization Act for fiscal year 2024 contains several provisions that will be implemented into law, including:

- Section 221: The DOD can now enter into agreements with eligible entities to assist universities in protecting sensitive research performed on its behalf, including engaging in vetting of visiting scholars, implementing research security standards, training on such requirements, and establishing and maintaining research security programs.

- Section 812: Requiring any covered consultancies that are receiving DOD funds to disclose potential ties to the governments of China and Russia, governments that sponsor terrorism, as determined by the Secretary of State, and entities subject to U.S. export controls and sanctions.[16]

Below is a list of other legislative proposals that have not yet advanced out of their relevant congressional committees:

Dump Investments in Troublesome Communist Holdings Act

Tax-exempt entities would lose their tax-exempt status if they hold any interest in a Chinese incorporated entity or any entity owned, directly or indirectly, by a Chinese entity.[17]

Protecting Endowments From Our Adversaries Act

All endowments with $1 billion in assets that invest in U.S. export restricted persons — which may be authorized currently — would be required to pay a 50% excise tax on the principal investment, and a

100% excise tax one year after an entity is designated.[18]

Preventing Malign CCP Influence on Academic Institutions Act

Universities would be required to (1) disclose gifts greater than $5,000 when provided by a Chinese-affiliated entity and all joint activities, including exchanges or research with such entities, and (2) publish all agreements with Chinese entities on their website.[19]

DHS Restrictions on Confucius Institutes and Chinese Entities of Concern Act

The U.S. Department of Homeland Security would be prohibited from providing funding to a university that (1) has a contract awarded, (2) enters into an agreement; or (3) receives an in-kind donation or gift from a Confucius Institute or any Chinese university that has certain affiliations with China's military or the Chinese Communist Party.[20]

Foreign Influence Transparency Act

This legislation would lower the financial threshold for reporting obligations under Section 117 of the Higher Education Act from $250,000 to $50,000.[21]

Finally, the Select Committee will continue to fully utilize its investigative powers throughout 2024. Universities will be a tempting target, as Congress has grown increasingly prone to hone in on universities, even if no specific violation has been identified.

Preparing for These Changes

As roles, responsibilities and controls expand, universities and research laboratories should take a more rigorous — and perhaps a more conservative — approach to research partnerships. What may be authorized or accepted today is liable to change on short notice, and could even hinder future funding opportunities.

Many of the proposed reviews from U.S. government agencies and Congress involve look-back processes that identify historical activity involving China or Russia, as opposed to only current or future activity.

Additionally, the traditional U.S. export controls exemption for fundamental research is being narrowed by the plethora of new regulations. Given the divergent expectations of competing compliance standards, universities and laboratories may opt to use the strictest regulations as their compliance standard.

In order to ensure universities and laboratories comply with these national security regulations, and to minimize reputational risk, universities should engage in talent-supply-chain due diligence by understanding their research collaborators.

Practically, this means confirming:

- Your researcher is not a U.S. export-restricted or sanctioned person, or part of any foreign talent program — malign or otherwise;

- Your research does not have any affiliations with U.S. export-restricted or sanctioned person, or with Chinese, Russian, Iranian or North Korean government entities. This could include any academic, professional or other appointments that have a monetary or other benefit or reward for the researcher.

- Your researcher does not have any "associations" with the above types of persons or government entities. This is essentially the same as "affiliations," but there is no type of reward or benefit provided — for example, co-publishing articles with such persons.

Moreover, universities and research institutions often operate in the public sphere, and managing reputational risks can be just as important to manage as legal risks. Developing a more rigorous compliance program can limit the likelihood of facing cases that may be permissible but could present reputational challenges.

Potential violations of regulations or laws should be thoroughly investigated, such that any investigation will be sufficient for regulatory, civil fraud, criminal law enforcement or congressional scrutiny. During an investigation, universities and laboratories should determine whether voluntary self-disclosure is warranted given the many benefits associated with such disclosures — and if so, to which agency, if not multiple agencies.

Michael K. Atkinson is a partner and the co-leader of the national security practice at Crowell & Moring LLP. He previously served as acting deputy assistant attorney general of the DOJ's National Security Division, and as the U.S. intelligence community inspector general.

Caroline Brown is a partner and the co-leader of the national security practice at the firm. She previously served in the DOJ's National Security Division and at the U.S. Department of the Treasury.

Jeremy Iloulian is counsel at the firm.

[1] https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.

[2] https://www.law360.com/articles/1585787/us-new-china-tech-unit-raises-domestic-research-scrutiny.

[3] https://www.justice.gov/opa/pr/justice-department-announces-five-cases-part-recently-launched-disruptive-technology-strike; https://www.justice.gov/opa/pr/russian-german-national-arrested-illegally-exporting-russia-sensitive-us-sourced; https://www.justice.gov/opa/pr/russian-international-money-launderer-arrested-illicitly-procuring-large-quantities-us; https://www.justice.gov/opa/pr/four-arrested-and-multiple-russian-nationals-charged-connection-two-schemes-evade-sanctions; and https://www.justice.gov/opa/pr/belgian-national-charged-crimes-related-scheme-illegally-procure-critical-us-technology-end.

[4] https://ofac.treasury.gov/media/932036/download?inline.

[5] The first tri-seal compliance note, issued in March 2023, focused on evasion of U.S. export controls and sanctions on Russia; https://www.bis.doc.gov/index.php/documents/enforcement/3240-tri-seal-compliance-note/file.

[6] https://www.crowell.com/en/insights/client-alerts/doj-ofac-and-bis-issue-tri-seal-compliance-note-focusing-on-voluntary-self-disclosures.

[7] https://www.crowell.com/en/insights/client-alerts/focusing-the-spotlight-doj-focuses-on-national-security-in-corporate-criminal-enforcement.

[8] https://www.justice.gov/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign.

[9] https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf.

[10] https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[11] https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

[12] https://www.crowell.com/en/insights/client-alerts/new-us-department-of-defense-policy-imposes-security-reviews-for-universities-and-labs-engaging-in-fundamental-research.

[13] https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-opens-investigation-university-dod-funded-weapons-research.

[14] https://selectcommitteeontheccp.house.gov/media/press-releases/alfred-university-closes-confucius-institute-results-select-committee.

[15] https://selectcommitteeontheccp.house.gov/media/letters/letter-uc-berkeley-joint-institute-linked-chinese-military.

[16] https://www.govinfo.gov/content/pkg/BILLS-118hr2670rh/pdf/BILLS-118hr2670rh.pdf.

[17] https://www.congress.gov/bill/118th-congress/house-bill/5109?s=1&r=25.

[18] https://www.congress.gov/bill/118th-congress/house-bill/4380.

[19] https://www.congress.gov/bill/118th-congress/house-bill/944/text?format=txt&r=22&s=1.

[20] https://www.congress.gov/bill/118th-congress/senate-bill/1121?q=%7B%22search%22%3A%22H.R.+2%22%7D&s=1&r=13.

[21] https://www.congress.gov/bill/118th-congress/house-bill/1819?s=1&r=97.