

Fundamental Research & National Security: Recent Developments & New Issues

by Nicole Engisch, Alex Hontos, Justin T. Huff, and Lawrence Ward

According to the National Center for Science and Engineering Statistics (“NCSES”), a key driver in the scientific and technological accomplishments of U.S. research universities is the volume of federal support for research and development (“R&D”). In FY 2021, the U.S. Government supplied some \$49 billion in R&D funding to U.S. institutions of higher education, and that contribution was 55% of total R&D spending in U.S. higher education.^[1] Of that federal contribution, the Department of Defense (“DoD”) supplied \$7.4 billion or about 15% of all such federal research funding.^[2]

Three different national security measures are likely to affect such federal funding of U.S. research institutions, their principal investigators (“PIs”) and their international research collaborations in the coming years: (1) the naming of more non-U.S. universities, academies, and institutes (particularly in China and Russia) to U.S. sanctions lists; (2) the DoD’s new efforts to mitigate undue foreign influence on DoD-funded research; and (3) the potential application of national security reviews under President Biden’s Executive Order 14105 (“EO 14105”) on future academic research collaborations with peer institutions and scholars in China in at least three particular fields of advanced technology – semiconductors, quantum computing, and artificial intelligence. In addition, national security critics are urging the President not to renew the historic 1979 framework agreement for scientific and technological cooperation with China.

1. Expansion of U.S. Sanctions Lists

U.S. Government agencies maintain and publish several lists under different statutory regimes to provide public notice that the listed individuals, entities, and organizations are “off-limits” for certain kinds of U.S. person activities or transactions (collectively, “Sanctions Lists”). For example, the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) administers and enforces the Trading with the Enemy Act (“TWEA”), the International Emergency Economic Powers Act (“IEEPA”), and the National Emergencies Act (“NEA”). Under various Executive Orders issued under these statutes, OFAC has created its Specially Designated Nationals and Blocked Persons List

Related People

- Nicole Engisch
- Alex Hontos
- Justin T. Huff
- Lawrence Ward

Related Capabilities

- National Security Law
- Government Enforcement & Corporate Investigations
- International Trade

(“SDN List”) and, more recently, its Non-Specially Designated Nationals Chinese Military-Industrial Complex Companies List (“Non-SDN CMIC List”). The U.S. Commerce Department’s Bureau of Industry and Security (“BIS”) enforces the Export Administration Act (“EAA”), the Export Control Reform Act (“ECRA”), and the Export Administration Regulations (“EAR”). Under these laws and regulations, BIS has its Denied Persons List (“DP List”), Unverified List (“UVL”), and Entity List (“Entity List”). Such Sanctions Lists have focused mainly on individuals (e.g., a wanted criminal), groups of persons (e.g., a known terrorist organization) or business enterprises (e.g., a front or sham company).

However in recent years, such U.S. agencies have also noted that, in certain adversary nations such as Russia or China, universities, academies, and institutes (collectively, “Foreign Institutions”) function essentially as extensions of their national governments. Thus, in those nations, such Foreign Institutions can become involved in the support of military, law enforcement, surveillance, or state-owned enterprise (“SOE”) activities. Where the U.S. agencies believe Foreign Institutions are involved in such activities to a degree deemed inconsistent with, or hostile to, U.S. national security or foreign policy interests, the U.S. agencies will also add Foreign Institutions to one or more of the Sanctions Lists.

OFAC has named over 170 Foreign Institutions in Russia to the SDN List, meaning that a U.S. person may not render any service or export anything to or receive any service or import from any Foreign Institution on the SDN List.^[3] OFAC has also designated at least one Foreign Institution in China - the China Academy of Launch Vehicle Technology - to its Non-SDN CMIC List. Strictly speaking, U.S. persons may not purchase or sell the public securities of entities on the Non-SDN CMIC List, but such a designation also conveys an official U.S. Government judgment that such a listed entity is part of the Chinese industrial military complex.

BIS has also named many Foreign Institutions in China to its Entity List, meaning that a BIS export license is required to export, reexport, or transfer certain items “subject to the EAR” to such a listed entity. Often, BIS will apply a “policy of denial” to review any license application, effectively barring any such cooperation or collaboration with such a listed Foreign Institution.^[4]

U.S. research universities and their PIs should therefore be prudent in selecting and managing their future international research collaborations and in screening potential collaboration partners to avoid dealing with a Foreign Institution on any Sanctions List. Such screening can be done through the Commerce Department’s Consolidated Screening List (“CSL”) online tool^[5] or through commercially available software applications. Using either method of screening, the U.S. university and its faculty and staff should maintain dated and retrievable records of the searches made in case a concerned federal funding agency later requests a review or audit.

2. The DoD’s Implementation of NSPM-33

In January 2021, President Trump signed National Security Presidential Memorandum 33 (“NSPM-33”)^[6] directing federal agencies to standardize their requirements for

federal research support regarding disclosure of conflicts of interest and conflicts of commitment (“COI/COC”) to mitigate the risks of undue foreign influence on, or illicit foreign access to, such research activity. After President Biden took office, his White House Office of Science and Technology Policy (“OSTP”) continued to support and implement NSPM-33 across the federal government.[7] OSTP convened key stakeholders, such as the DOD, the National Science Foundation (“NSF”), and the National Institutes of Health (“NIH”), to develop and issue harmonized policies on disclosures by PIs and funded institutions about their COI/COC situations.

On June 8, 2023, the DoD, acting through the Under Secretary of Defense for Research and Engineering, issued its “*Policy for Risk-Based Security Reviews of Fundamental Research*” (“Review Policy”)[8] in furtherance of NSPM-33 and to carry out the direction of Congress in Section 1286 of the John S. McCain National Defense Authorization Act of 2019 (“2019 NDAA”).[9] The Review Policy has several goals: (a) to assure the integrity of DoD-funded research; (b) to compel institutions and PIs to make full and timely disclosure of potential COI/COC situations to the relevant DoD component that is to provide the research funding; and (c) to communicate to institutions and PIs what relationships or conduct are likely to raise research security concerns for such DoD research funding, such as participation in foreign “talent” programs or receipt of other research funding from a “country of concern.” The Review Policy expressly names China, Russia, Iran, and North Korea as such “countries of concern.”

The Review Policy directs the DoD funding components to implement new risk-based security review processes to standardize COI/COC disclosure requirements across all DoD funding components and to identify proposals needing risk mitigation before awarding federal research funds. The Review Policy also includes a new explicit decision matrix that DoD funding components must now apply to determine when mitigation is required or recommended. At the same time, the Review Policy indicates that the DoD components are to carry out these new directives so as not to discourage international research collaborations or to unreasonably extend the DoD decision period for awards (but the additional time needed for the development and implementation of needed risk mitigation measures will not be counted as award time).

The Review Policy thus gives U.S. institutions of higher education and their PIs a new tool to assess their COI/COC disclosure obligations and the security risks that may flow as a result of relationships with foreign governments. The Review Policy also offers various risk mitigation techniques that U.S. institutions can adopt. Those techniques include “insider threat” identification training for PIs, a requirement of more frequent COI/COC disclosure, removal or replacement of PIs deemed to be security risks, and more institutional supervision of foreign commitments or activities by PIs along with clearer authorization for an institution to block certain commitments or activities deemed to pose undue security risks.

Most, if not all, U.S. institutions of higher education – even if they have little or no DoD research funding – could benefit from studying the Review Policy because it reveals how the U.S. Government will perceive and evaluate research security risks. The Review

Policy is essentially a bellwether for how the U.S. Government wants NSPM-33 to be implemented across the federal government, helping institutions to update, adapt, and modify their award application management processes and research security procedures in line with the U.S. Government's expectations. Some key "take-aways" in the Review Policy include suggestions such as:

- Adopt and implement clear COI/COC policies and procedures to identify and address any on-campus research funded by a foreign government or any joint or visiting appointments of investigators by Foreign Institutions, especially if such institutions are funded and managed by a foreign government.
- Communicate such COI/COC policies and procedures widely and clearly across the whole institution to all faculty, staff and students, and retrain them accordingly.
- Candidly consider if a proposed research collaboration may involve any of the "countries of concern" as identified in the Review Policy or a Foreign Institution on any Sanctions List, and, if so, apply enhanced due diligence and risk management procedures in light of the additional compliance risks and obligations that are likely to come with such collaborations.
- Continue to affirm and validate the central values of U.S. higher education, such as academic freedom, open publishable research, and the free international flow of scholarship and scholars.

3. The Potential Intrusion of Executive Order 14105

On August 9, 2023, President Biden issued Executive Order 14105 ("EO 14105") on *Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern* to provide a new mechanism to limit certain outbound U.S. investments to "countries of concern." The EO 14105 Annex defines "countries of concern" as the People's Republic of China and its Special Administrative Regions of Hong Kong and Macau (collectively, "China").

EO 14105 directs the Secretary of the Treasury, together with the Secretary of Commerce and other Cabinet members, to adopt a new two-part program to regulate outbound investments regarding "covered national security technologies and products." Currently, as set out in EO 14105, that key phrase is limited to certain (a) semiconductors and microelectronics; (b) quantum information technologies; and (c) artificial intelligence ("AI") sectors that are critical for China's military, intelligence, surveillance, or cyber-enabled capabilities.

On August 14, 2023, the U.S. Department of the Treasury ("Treasury") published an advance notice of proposed rulemaking ("ANPRM") to carry out EO 14105.^[10] As envisioned in EO 14105 and the ANPRM, the new program will include both the required notification to Treasury of some covered transactions and the outright prohibition by Treasury of certain other covered transactions. EO 14105 reinforces the new regulations by prohibitions against conspiracy and evasion of the new reporting requirements and prohibitions and also authorizes the Secretary of the Treasury to prohibit a U.S. person from knowingly directing transactions to others that a U.S. person could not lawfully perform and to require notification of transactions or to prohibit transactions that would

be accomplished through any U.S. person-controlled foreign entity.

This striking language appears in the middle of the 14-page Federal Register announcement of Treasury's ANPRM under EO 14105[11]:

The Treasury Department does not intend the definition of “covered transaction” under consideration to apply to the following activities, so long as they do not involve any of the definitional elements of a “covered transaction” and are not undertaken as part of an effort to evade these rules: university-to-university research collaborations; ... intellectual property licensing arrangements; ...

Taken at face value, the above Treasury statement might reassure U.S. institutions of higher education and their PIs because Treasury says this new regulatory system is not intended to apply to “university-to-university research collaborations” or “intellectual property licensing arrangements” between the United States and parties in China. However, by its terms, the ANPRM's statement of intention is not absolute; rather, it is explicitly conditioned on two factors: (1) the collaboration or licensing arrangement must not involve any of the definitional elements of a covered transaction as defined in EO 14105 and the ANPRM, and (2) the collaboration or licensing arrangement is not “part of an effort to evade these [new] rules.” Accordingly, for a U.S. institution of higher education to safely conclude it is outside these new rules, it would likely need to review all the relevant facts and circumstances of any such U.S.-China research collaboration or licensing arrangement in light of these new proposed Treasury regulations.

Later, on the same page of the Federal Register notice, Treasury expressly asks for public input on whether the proposed regulations should include “additional clarity” regarding what constitutes a “covered transaction” that is either prohibited or that must be notified to Treasury, given that Treasury's stated goal is not to pick up “university-to-university research collaborations” or “intellectual property licensing arrangements” except when “undertaken as part of an effort to evade these rules.” It will be instructive to see how much greater certainty or clarity from Treasury can be achieved by the U.S. higher education community and its representative organizations to avoid being drawn into these potentially complex regulatory issues. If the final regulations lack clear “bright line” standards to eliminate doubt or uncertainty, there may be many inevitable frictions and delays to ordinary and routine scientific research in these burgeoning fields by collaborators in the United States and China or to ordinary and routine technology transfer transactions by U.S. universities involving university-owned patents.

Importantly, in issuing EO 14105, President Biden invoked the IEEPA as its main legal basis, which imposes a maximum civil penalty of the greater of two times the transaction value or \$356,579 (as of January 13, 2023). In addition, under IEEPA, a willful commission, willful attempted commission, willful conspiracy to commit, or aiding or abetting in the commission of a violation of any license, order, regulation, or prohibition may, upon conviction, lead to criminal fines of not more than \$1,000,000, or if a natural person is involved, imprisonment for not more than 20 years, or both. Thus, even the potential application of these new outbound investment regulations to U.S. university research collaborations or intellectual property licenses with Chinese counterparties

could become burdensome and pose significant legal and financial risks to certain scientific research cooperation between the United States and China.

4. 1979 Science and Technology Agreement.

After President Carter normalized diplomatic relations with China in 1979, the United States and China entered into a science and technology agreement (“STA”) to provide a framework for mutually beneficial research cooperation. The STA did not specify any particular type or form of research or allocate any funds. Nonetheless, it set a foundation for many fruitful collaborative efforts (e.g., in nutrition, public health and other such fields) and had been renewed under both Democratic and Republican administrations every five years for over four decades.

However, recently, some legislators in both houses of Congress have urged the White House to scrap the STA because of fears that such collaborative research leading to “dual-use” scientific or technological discoveries may enhance the modernization of China’s military or other security forces. When the current STA was about to expire in August 2023, the Biden Administration reacted cautiously, not abandoning the STA altogether but also not renewing it for another five-year term. Instead, the U.S. State Department announced the STA would be extended for six months to allow time for the two governments to negotiate further safeguards for U.S. national and economic security interests.^[12] Whether the Administration ultimately renews the STA or allows it to lapse will be another strong harbinger for U.S. research universities regarding the geopolitical climate for collaborative scientific research between the United States and China.

5. Conclusion

The ongoing geopolitical tensions between the United States and its main strategic adversaries China and Russia continue to ripple across many aspects of federal policy. In this paper, we have examined three different but interrelated measures by the U.S. Government to protect national security that are likely to affect U.S. research universities. U.S. institutions of higher education and their PIs will need to be more astute in their selection of international research topics and partners, especially when dealing with peer institutions or scholars in “countries of concern” such as China or Russia, to avoid collaborations with Foreign Institutions on any Sanctions Lists. They will also need to understand not only the risks that may impact their continued eligibility for federal R&D funding but also potential civil penalties and even criminal prosecution they may face for incomplete or untimely COI/COC disclosures as required by NSPM-33 and its implementing measures, such as the newly announced Review Policy for DoD research awards. Treasury’s new outbound investment reviews under EO 14105 may potentially add a further layer of complexity and legal exposure to such international research collaborations or technology transfer transactions between the United States and China. Finally, universities and PIs should take note if the Biden Administration chooses to renew or abandon the STA with China by the time its temporary six-month extension ends in February 2024.

[1] <https://ncses.nsf.gov/pubs/nsf23303#:~:text=Universities>.

[2] *Id.*

[3] Among others, those OFAC SDN List designations of Foreign Institutions in Russia include 33rd Scientific Research and Testing Institute, All-Russian Scientific Research Institute of Aviation Materials, Central Scientific Research Institute of Automation and Hydraulics, Research and Design Institute for Thermal Engineering, Molecular Electronics Research Institute, V.V. Bakhirev Scientific Research Institute for Mechanical Engineering, the V. Tikhomirov Scientific Research Institute for Instrument Design, and Scientific Research Institute of Organic Chemistry and Technology.

[4] Among others, these BIS Entity List designations of Foreign Institutions in China include Beihang University (formerly known as Beijing University of Aeronautics and Astronautics), Beijing University of Posts and Telecommunications, China Academy of Electronics and Information Technology, China Haiying Electro-Mechanical Technology Academy, Beijing Institute of Radio Measurement, Beijing Institute of Remote Sensing Equipment, the Beijing Institute of Computer Applications and Simulation Technology, Beijing Institute of Environmental Features, the Shanghai Academy of Spaceflight Technology, Shanghai Institute of Space, Guangzhou Institute of Communications, North China Research Institute of Electro-Optics, Hebei Semiconductor Institute, Nanjing Research Institute of Electronics Technology, Southwest China Institute of Electronics, East China Research Institute of Electronics Engineering, China Ship Research and Development Academy, Chinese Academy of Engineering Physics, Harbin Institute of Technology, Nanjing University of Science and Technology, Northwestern Polytechnical University, Sichuan University, and Tianjin University.

[5] <https://www.export.gov/consolidated-screening-list>

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

[7] <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

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

[9] Pub. L. 115-232.

[10] “Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern,” 88 Fed. Reg. 54961 (Aug. 14, 2023).

[11] *Id.*, at 54965.

[12] <https://www.science.org/content/article/white-house-requests-extension-agreement-china-joint-research>