Statement of the Association of American Universities

"Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise"

Hearing before the
Committee on Science, Space, and Technology
U.S. House of Representatives

February 15, 2024

The Association of American Universities (AAU), America's leading research universities, commends the House Committee on Science, Space, and Technology for everything it has done to help bolster the security of federally funded research and to protect against undue foreign influence. We greatly appreciate the committee's willingness to work with the university and the research community to protect and preserve the scientific openness that has been critical to U.S. leadership in science and technology while at the same time making sure that steps are taken to prevent foreign actors from taking advantage of that openness. We also acknowledge and appreciate the committee's interest in exercising its oversight role regarding research security and for holding today's hearing on "*Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise*."

America's leading research universities take seriously both international scientific collaboration and the economic and national security threats posed by foreign adversaries. Theft of intellectual property directly affects universities, which, under the Bayh-Dole Act of 1980, maintain rights to the intellectual property they produce from federally funded research discoveries. IP theft can therefore result in significant monetary losses for universities as well as risks to America's national and economic security.

Over the last several years, universities have been actively working to inform their researchers about possible risks associated with contracts and agreements with entities from specific foreign countries, educate them about potentially malign foreign talent programs, and to ensure that they properly disclose to their institution and federal research agencies their relationships and funding received from outside foreign sources. AAU staff along with our 69 U.S.-based member universities and other associations have also been working closely with federal research agencies and intelligence agencies, including the Federal Bureau of Investigation (FBI), to better understand threats posed by foreign actors in order to mitigate risk and address research security concerns on campus.

Indeed, universities are working every day to secure and protect the integrity of the research they conduct on behalf of the federal government from threats posed by malign foreign actors. Actions taken include:

> ***Research Security Strategy and Coordination***: Universities have established campus-wide working groups and task forces on research security which regularly meet to review the latest threats and effective practices and discuss policy implementation. Institutions have also established a chief

research security officer position to coordinate and oversee campus efforts to protect and secure research.

Research Faculty Awareness Building Efforts: Universities have created centralized websites and increased direct faculty communications to make sure that they fully understand current federal disclosure requirements related to research security and risks associated with certain international collaborations.

Risk Assessment and Mitigation Review Process: Universities have developed risk criteria and use of comprehensive review processes for review of grants, contracts, and foreign gifts. To this end, some institutions have established new risk management committees for discussion and review of international engagements and collaborations.

Research Security Training Requirements: Now that the National Science Foundation (NSF) has released the completed research security training modules[1] as required by the CHIPs and Science Act of 2022, institutions are incorporating the modules into existing training platforms and requirements. The training modules help provide a baseline understanding of research security concerns across the research enterprise which re. Some institutions are also providing additional training to researchers whose research has been identified as potentially more vulnerable to security breaches or foreign malign influence.

Policies on Disclosure of Conflicts of Interest, Conflicts of Commitment and Foreign Funding Sources: Universities have reviewed their conflict of interest and conflict of commitment policies and made updates to faculty disclosure policies to more clearly identify foreign affiliations, relationships, and financial interests.

Engagement and Coordination with Federal Intel Agencies and Security Officials: Universities regularly meet and have built strong relationships with their local FBI offices. Universities also engage research funding agencies when they need to mitigate and resolve a research security issue.

Policies on Foreign Gifts and Contracts Reporting: Universities have assessed their policies on reporting foreign gifts and contracts and have improved their reporting procedures as part of Section 117 of the Higher Education Act.

Policies on International Travel: Universities have developed new risk-based international travel policies for faculty and staff, some require researchers to pre-register their foreign travel. Importantly, many institutions offer tailored training briefings to specific faculty before they travel to destinations considered high-risk. For those faculty, universities help mitigate risks by providing secure loaner laptops and encouraging faculty to not cross international borders with devices containing research data.

[1] NSF research security training modules now available, January 30, 2024: https://new.nsf.gov/news/nsf-research-security-training-modules

Policies on International Visitors to Campus: Universities have developed requirements for vetting and securely hosting foreign visitors while on campus including centralized processes for evaluating prospective visitors against restricted party lists, U.S. sanction programs, export controls, and other research security topics.

Policies on Export Control Compliance: Universities have comprehensive policies regarding whether and how they will undertake export-controlled research activities. This includes using restricted party screening software within shipping, procurement, and academic visitor processes. Additionally, universities have an export control officer (or officers) with overall responsibility for ensuring university compliance with export control rules and other security controls. On many campuses, faculty training to ensure compliance with export controls requirements is already in place.

Cybersecurity Protocols: Universities have identified appropriate protections for sensitive data in grants and contracts to ensure compliance with NIST SP 800-171. More than 600 institutions are also part of the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) which monitors the threat landscape and shares threat information with its network. Institutions have also taken measures to improve data security and use encryption, multi-factor authentication, and virus scanning tools.

Congress has also enacted several provisions to address research security through the CHIPS and Science Act of 2022 and the National Defense Authorization Act.[2] Our universities have and will continue to work to ensure compliance with these congressional requirements.

Starting from language in the FY2020 National Defense Authorization Act,[3] which mandated the creation of the National Science and Technology Council's (NSTC) interagency subcommittee on research security, NSPM-33 and its implementation guidance specifically called for the effective coordination and harmonization of research security requirements across federal research agencies. This includes the recent finalization of common disclosure elements and forms.[4]

AAU, along with several other higher education associations, research organizations, and universities, also submitted extensive comments[5] to OSTP's request for information[6] on the draft research security program guidance.[7] AAU's comments, similar to several other submitted comments, described significant concerns with the lack of a risk-based approach to research security and the need for clear

[2] University and Federal Actions Taken to Address Research Security Issues, updated January 4, 2024: https://www.aau.edu/key-issues/university-and-federal-actions-taken-address-research-security-issues
[3] Securing American Science and Technology Act (SASTA), Section 1746 of the FY20 NDAA (P.L. 116-92)
[4] NSTC Research Security Subcommittee, NSPM-33 Implementation Guidance, Disclosure Requirements & Standardization: https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp
[5] AAU Submits Response to OSTP Request for Information on NSPM-33, May 31, 2023: https://www.aau.edu/key-issues/aau-submits-response-ostps-request-information-nspm-33
[6] Request for Information; NSPM-33 Research Security Programs Standard Requirement, March 7, 2023: https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement
[7] Subcommittee on Research Security, National Science and Technology Council, Office of Science and Technology Policy, DRAFT Research Security Programs Standard Requirement, February 2023: https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

and consistent guidance across research agencies when implementing research security program requirements. However, since the June 2023 comment deadline, OSTP has not yet released final requirements or an update to the research community on the status of finalizing the requirements. We are hopeful that by issuing final guidance, OSTP and other federal agencies will take seriously concerns AAU and other associations have raised in the comments to ensure that any final guidance is both risk-based and harmonized across federal agencies. Significant variation in what agencies require for acceptable research security programs will make compliance difficult and would not be in our national interest.

As the threats to the research environment continue to evolve, we look forward to continuing to engage with the committee on issues related to research security and share how America's leading research universities are approaching these issues. Thank you again for holding this important hearing.