Actions Taken to Address Foreign Security Threats, Undue Foreign Interference, and Protect Research Integrity at U.S. Universities

Congress is currently considering several measures related to securing federally funded research data and intellectual property at universities and other research institutions in the United States. As lawmakers consider these measures, it is important to understand the current state of play for research security in the country to avoid new requirements that are duplicative, unnecessary, or counterproductive. Below is a summary of actions that have already been taken or are currently being taken by both universities and federal entities regarding research security.

Actions Taken by Universities

- Research universities take seriously national security threats posed by international actors. Universities have a vested interest in protecting intellectual property, proprietary information, trade secrets and classified and/or otherwise controlled government information housed at universities. To address these issues, universities have taken steps to protect the research they conduct, including:

   o Strengthening institutional conflict-of-interest (COI) and conflict-of-commitment (COC) requirements.
   o Enhancing communications and training for researchers on security threats and institutional and federal security requirements.
   o Enhancing campus coordination efforts.
   o Enhancing scrutiny of research activities and partnerships with foreign entities.
   o Enhancing reviews of international collaborations, contracts, and foreign gifts.
   o Implementing safeguards and protections for researchers on foreign travel.
   o Enhancing cybersecurity efforts and training.
   o Increasing and better coordinating with the FBI and other government security agencies to identify, and mitigate, potential threats.

- AAU and APLU have conducted two surveys of their member institutions to identify effective practices universities have taken to address threats and concerns.

- AAU and APLU have also developed principles and values to guide actions relevant to foreign government interference in university research.

AAU, along with other higher education associations and universities, have been supportive of several congressional and administrative actions taken to address foreign threats to research, including the following provisions:

- **Section 1286 of the National Defense Authorization Act for Fiscal Year 2019** required the Secretary of Defense to establish an initiative to work with institutions of higher education who perform defense research and engineering activities and name an academic liaison. Also requires DOD to publish a list of Chinese institutions. This requirement was further modified and updated in **Section 1281 of the National Defense Authorization Act for Fiscal Year 2020** to support protection of national security academic researchers from undue influence and other security threats.

- **Section 1746 of the National Defense Authorization Act for Fiscal Year 2020** required OSTP to establish an interagency working group (the JCORE Research Security Subcommittee) under the National Science and Technology Council (NSTC) to protect federally funded research and development from foreign interference, cyberattacks, theft, or espionage and to develop recommendations for best practices for federal agencies and grantee institutions. The JCORE Research Security Subcommittee's work resulted in the issuance in January 2021 of a [Presidential Memorandum on United States Government-Supported Research and Development National Security Policy](#) (NSPM-33) and the White House OSTP/NSTC report on "[Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Enterprise](#)."

- **Section 1746 of the National Defense Authorization Act for Fiscal Year 2020** called on the National Academy of Science, Engineering and Medicine to stand up a new [Roundtable on Science, Technology, and Security](#) to bring together key stakeholders from the scientific enterprise (including federal agencies, universities, and industry) to enter into a constructive and ongoing dialogue on research security. The Roundtable has now held several [meetings](#) since it began its work on November 2020.

- **Section 223 of the National Defense Authorization Act for Fiscal Year 2021** mandates disclosure of funding sources in applications for federal research and development awards for all federal research agencies. Additionally, universities are held accountable for ensuring faculty are aware of these disclosure requirements.

- **Section 1299C of the National Defense Authorization Act for Fiscal Year 2021** (modifying Sec. 1286 from the FY19 NDAA and Sec. 1281 of the FY20 NDAA) requires the

Secretary of Defense and other government agencies to establish an initiative to protect researchers from undue influence and other security threats, support protection of intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security, including by:

- The required publication of a list of "foreign talent programs" and a list of academic institutions in countries, including China and Russia, that have engaged in various malicious practices or that "operate under the direction of the military forces or intelligence agency of the applicable country."
- The required designation of an official responsible for liaising with academic institutions and briefing them on espionage risks.

- **Section 1062 of the National Defense Authorization Act for Fiscal Year 2021 and Section 10339A of the CHIPS and Science Act of 2022** restricts DOD and NSF funds to institutions that host a Confucius Institute.

- **Section 9907 of the National Defense Authorization Act for Fiscal Year 2021**), prohibits any funds appropriated for its microelectronics initiatives and incentives to be provided to a "foreign entity of concern"; defined broadly, to include nationals of certain countries.

- The **CHIPS and Science Act of 2022** included several research security measures:
  - **Section 10114** required DOE to develop and maintain tools and processes to manage and mitigate research security risks, such as the science and technology risk matrix
  - **Sections 10331 to 10336** established a Research Security and Policy Office at NSF
  - **Section 10337** updated responsible conduct in research training to raise awareness of potential security threats, and federal export control, disclosure, and reporting requirements. **Section 10634** requires institutions and researchers to certify training has occurred as part of the application for a research award.
  - **Section 10338** establishes a Research Security and Integrity Information Sharing Organization to help universities and researchers identify improper and illegal efforts
  - **Section 10339** requires NSF to develop a plan to identify research areas, including key technology areas, that may involve access to controlled unclassified or classified information
  - **Section 10339B** requires institutions to annually provide a summary report to NSF current financial support, including gifts and contracts, of $50,000 and above from foreign countries of concern
  - **Section 10631 and 10632** prohibits all agency personnel from participating in a malign foreign talent recruitment program and required OSTP to distribute a

uniform set of guidelines for federal research agencies regarding foreign talent recruitment programs. Also required individuals to certify they are not part of a malign foreign talent program and that policies developed should not prohibit activities related to international collaborations

- **The SBIR and STTR Extension Act of 2022** requires agencies to implement a due diligence program to assess security risks for all SBIR and STTR proposals. Requires disclosure of information related to foreign ties, business relationships, investment, and ownership.

Actions Taken by the Executive Branch and Federal Agencies

- NSPM-33 Research Security Program Standards: In March 2023, the White House Office of Science and Technology Policy (OSTP) in coordination with the National Science and Technology (NSTC) Subcommittee on Research Security released the draft research security programs standard requirement for public comment. The new research security program standards require institutions with federal research portfolios of $50M or more per year to maintain an international travel policy, implement research security training, implement baseline safeguarding protocols and procedures for information systems used to store, transmit, and conduct federally funded R&D, and provide training to relevant personnel on export control procedures and requirements. Final requirements are expected later in 2023.

- NSPM-33 Common Disclosure Forms: In August 2022, the White House Office of Science and Technology Policy (OSTP) in conjunction with National Science and Technology (NSTC) Subcommittee on Research Security, developed and released for comment standardized disclosure requirements as part of the administration implementation of NSPM-33. The objective of the disclosure requirements if to "provide clarity regarding disclosure requirements, disclosure process, and expected degree of cross-agency uniformity." Forms are expected to be finalized in 2023.

- NSPM-33 Implementation Guidance – In January 2022, the White House Office of Science and Technology Policy (OSTP) and the National Science and Technology (NSTC) Subcommittee on Research Security issued guidance to Federal departments and agencies regarding the implementation of National Security Presidential Memorandum-33 (NSPM-33). Among other things, the guidance requires universities receiving more the $50 million in federal research funds annually to develop comprehensive research security plans focused on: cyber security, foreign travel security, insider threat awareness and research security training, and export control training and compliance. The guidance also seeks to assist research agencies in harmonizing requirements that

federally funded university researchers disclose any funding or in-kind support they receive from both foreign and domestic sources.

- NSF has issued clarifications to its proposal disclosure requirements to ensure proposers provide information on all sources of current and pending research support. The agency has also revised their Proposal and Awards Policies and Procedures Guide (PAPPG), providing the community with a standardized format for disclosure information. NSF has convened research integrity roundtables with researchers. The agency has also created a new position of Chief of Research Security and Policy.

- DOE, DOD, and NSF have prohibited agency personnel from participating in a foreign talent recruitment program.

- NIH has issued clarifications of the biosketch, other support, and application form instructions as well as hosted events to answer questions.

- The FBI has convened two large academic summits as well as several other regional events to foster engagement and information sharing between universities and intelligence and security officials. Additionally, FBI regional offices have actively engaged with academic institutions in their regions on a more regular and consistent basis to ensure research security and integrity.

Existing Federal Research Security Requirements

- **Controlled Unclassified Information (CUI)** – The U.S. has established a process for regulating and securing various categories of controlled unclassified information (CUI) resulting from research and other non-classified information that requires safeguarding or dissemination controls pursuant to E.O. 13556 of Nov 4, 2010. 32 CFR Part 2002 identified that prior to the process established for CUI under E.O. 13556 of Nov 4, 2010 "agencies often employed ad hoc, agency-specific policies, procedures, and markings to handle this information. This patchwork approach caused agencies to mark and handle information inconsistently, implement unclear or unnecessarily restrictive disseminating policies, and create obstacles to sharing information."

- **Export Control/Deemed Export Regulations** – There are multiple sets of regulations in effect regarding control of specific types of technology and data services for export, including the release of controlled technology to foreign persons in the U.S. known as "deemed" exports. Regulations include:

- Department of Commerce requirements under 15 CFR Part 730-774, which oversees the Export Administration Regulations (EAR) to control dual-use technology on the Commerce Control List (CCL);
- Requirements from the State Department's Directorate of Defense Trade Controls under 22 CFR Parts 120-130, which oversees the International Traffic in Arms Regulations (ITAR) and controls items designed and developed for military use on the U.S. Munitions List;
- Requirements from the Treasury Department's Office of Foreign Assets Controls (OFAC) under 31 CFR Parts 501-598, which controls interactions with nations against which there are U.S. trade embargoes (e.g. Cuba, Iran, Syria, North Korea, Myanmar and Sudan); and
- the Nuclear Regulatory Commission under 10 CFR Part 110, which oversees controls on the export and import of nuclear equipment and materials.

- **Dual Use Research Concerns (DURC)** – Control of Select Biological Agents and Dual Use Research of Concerns (DURC) is overseen by the U.S. Department of Health and Human Services and the U.S. Department of Agriculture under 7 CFR 331, 9 CFR 121, 42 CFR 73.

- **HEA Section 117** – Institutions are required to disclose foreign gifts and contracts above $250,000 as mandated under 20 U.S.C. § 1011f and in accordance with Section 117 of the Higher Education Act.