last updated February 2025

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:
    - Strengthening institutional conflict-of-interest (COI) and conflict-of-commitment (COC) requirements.
    - Enhancing communications and training for researchers on security threats and institutional and federal security requirements.
    - Enhancing campus coordination efforts.
    - Enhancing scrutiny of research activities and partnerships with foreign entities.
    - Enhancing reviews of international collaborations, contracts, and foreign gifts.
    - Implementing safeguards and protections for researchers on foreign travel.
    - Enhancing cybersecurity efforts and training.
    - 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.

Actions Taken by Congress

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** requires 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. Additional modifications were made in **Section 1223 and 1224 of the National Defense Authorization Act for Fiscal Year 2024** to require a report on the implementation of Section 1286 policies and procedures as well as NSPM-33 by July 2025. The addition also requires DOD to notify an individual suspected of knowingly engaging with entities identified on the Section 1286 list, establishes an appeals procedure, and an annual compliance certification requirement. **Section 226 and Section 238 of the National Defense Authorization Act for Fiscal Year 2025** added requirements for DOD to conduct periodic examinations of research awards to ensure compliance with current DOD research security policy and prohibits DOD funding to institutions of higher education that conduct fundamental research in collaboration covered entities identified on the Section 1286 list.

- **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 held 14 meetings between November 2020 and May 2024, culminating with a capstone workshop held in July 2024. Proceedings from the capstone workshop were released in January 2025.

- **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. Additionally, **Sections 1044 and 1045 of the National Defense Authorization Act for Fiscal Year 2024** made modifications to the definition of a Confucius Institute and terminated DOD's authority to issue a waiver to institutions who maintain 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: In January 2021, the White House released National Security Presidential Memorandum 33 (NSPM-33) directing agencies to take action to strengthen protections of U.S. government-supported research and development against foreign government interference and exploitation. In January 2022, additional guidance was issued 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.

- 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." The forms were finalized at the end of 2023 and OSTP released a memorandum to federal research agencies in February 2024 requiring the use of the harmonized common disclosure form.

- NSPM-33 Research Security Plans: In July 2024, the White House Office of Science and Technology Policy (OSTP) issued additional guidance to federal research agencies in July 2024 for implementation of the NSPM-33 requirement for research security plans. The guidance requires institutions of higher education that receive more than $50 million in federal research funding to certify that they have implemented their own research security programs, which include training for cybersecurity, research security and export control as well as periodic training on foreign travel security for covered individuals engaged in international travel and implementing a travel reporting program. Within 6 months of the memorandum, federal research agencies were to submit to OSTP and OMB plans for updating their policies to ensure the guidance is reflected in their own requirements. Updated policies are to take effect no later than 6 months after finalized plans have been submitted and provide adequate time (but not more than 18 months) for institutions to implement the requirements.

- Department of Defense: DOD issued a policy in July 2023 for risk-based security reviews of fundamental research. As part of this policy, a list of institutions and foreign talent programs which pose a threat to the national security interests of the U.S. was made publicly available.

- National Science Foundation: NSF created a new Office of Research Security and Policy in 2022. In June 2024, NSF announced a new risk mitigation process, the Trusted Research Using Safeguards and Transparency (TRUST) framework, which will guide the agency in assessing grant proposals for potential national security risks. The TRUST process will be rolled out in three phases, beginning in FY25 with a pilot on quantum-related proposals. Additionally, in July 2024, NSF announced a five-year $67 million investment establishing the Safeguarding the Entire Community of the U.S. Research Ecosystem (SECURE) Center. The SECURE Center will share information and reports on research security risks, providing training on research security to the science and engineering community and serve as a bridge between the research community and

government funding agencies to strengthen cooperation on addressing security concerns.

- Department of Energy: DOE established the Office of Research, Technology, and Economic Security (RTES) in October 2022 to support the Department's programs in due diligence reviews and risk mitigation. In November 2024, DOE announced their framework for financial assistance and loan activities in order to make risk-based investment decisions and ensure transparency.

- National Institutes of Health: NIH issued a decision matrix in August 2024 for assessing potential foreign interference as part of its ongoing efforts to be transparent about its policies and procedures. The matrix includes details on the process NIH takes to handle new allegations of foreign interference, and also offers details as to how NIH considers whether to contact institutions to request additional information.

- Foreign Talent Recruitment Programs: DOE, DOD, and NSF have prohibited agency personnel from participating in a foreign talent recruitment programs. Additionally, as part of the CHIPS and Science Act, OSTP was tasked with publishing and widely distribute a uniform set of guidelines for Federal research agencies regarding foreign talent recruitment programs. Those guidelines were released in February 2024.

- Intelligence Community Engagement: Since 2018, 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.