ASSOCIATION OF
PUBLIC &
LAND-GRANT
UNIVERSITIES

June 1, 2023

VIA Email: researchsecurity@ostp.eop.gov
The White House
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

ATT: Comment on Request for Information; NSPM 33 Research Security Programs Standard Requirement (88 FR 14187)

To Whom it May Concern:

On behalf of the Association of Public and Land-grant Universities (APLU), we thank you for the opportunity to provide input on the draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33.

APLU is a research, policy, and advocacy organization dedicated to strengthening and advancing the work of public universities. With a membership of more than 250 public research universities, land-grant institutions, state university systems, and affiliated organizations, APLU's agenda is built on the three pillars of increasing degree completion and academic success, advancing scientific research, and expanding engagement. Annually, our U.S. member campuses enroll 4.2 million undergraduates and 1.2 million graduate students, award 1.2 million degrees, employ 1.1 million faculty and staff, and conduct $48.7 billion in university-based research.

The nation’s public research universities have a unique and long-standing partnership with the federal government conducting research on behalf of the American people. This research represents one of the nation’s greatest assets, which is why foreign governments may attempt to take advantage of our open and collaborative research ecosystem. APLU has worked with federal agencies and our member institutions to identify and share best practices to help protect against foreign government interference, influence, and theft of research and innovative discoveries. In furtherance of securing research, APLU has surveyed our member universities on research security practices, held work sessions to advance best practices in the field and further understanding of the problems that must be addressed, and hosted numerous federal agency officials at association meetings to enhance collaboration between the academic and security agency communities to achieve common objectives. While increasing research security measures, our institutions are simultaneously working to ensure that they remain open and inviting to attract the best minds and ideas from throughout the world.

APLU appreciates the work of the White House Office of Science and Technology Policy to focus on the three Administration priorities in the area of research security and integrity, including protecting America's security and openness, providing clear guidance with minimally burdensome regulation, and importantly, ensuring policies do not fuel xenophobia or prejudice. APLU worked with our colleagues at AAU, AAMC, ACE, AUECO, COGR, and EDUCAUSE in analyzing proposed Standard Requirements, and each group will be commenting individually around complimentary themes. APLU provides comments on five areas regarding the proposed Research Security Programs Standard Requirement identified in the Request for Information as follows:

1. Equity

   NSPM-33 calls on research organizations "that have received at least $50 million per year in Federal science and engineering support for each of the previous two consecutive fiscal years" to maintain a certified research security program. This threshold likely recognizes that maintaining a certified research security program could be difficult for less resourced institutions. **The Standard Requirement should provide more clarity regarding the calculation of the $50 million threshold to include a single federal source for the calculation and notice to covered institutions.** In addition, institutions may have research levels that regularly fluctuate around the threshold level, and the Standard Requirement should clarify the timeline to comply with the Standard Requirement for institutions that newly reach the threshold. For instance, the Standard is not clear on the timeframe for newly covered institutions. These institutions should also be given a year to come into compliance as is currently envisioned for covered institutions upon enactment of the Standard.

   APLU analyzed its membership and identified approximately half of its member institutions could be considered a covered research organization. A significant portion of R2 classified institutions and Minority Serving Institutions, including Historically Black Colleges and Universities, would not currently be covered in the proposed policy. **OSTP should make clear in agency guidance that institutions under the $50 million threshold should not be penalized in future funding or be disqualified from any solicitation because their institution does not self-certify a research security plan (although some institutions may choose to do so or be required if they engage in CUI or classified research).** Faculty at non-covered institutions will still need to follow all regulations related to disclosure of outside support and required research security training called for in other regulations.

   On the issue of non-discrimination, APLU remains concerned about the terminology of "insider threat" with regard to research security training. **Insider threat terminology is not regularly**

used in academia outside of controlled unclassified information or classified research. APLU members have suggested OSTP should use the term "insider risk" as it may be more appropriate for the fundamental research space. However, regardless of the terminology used, it should be stated clearly in the standards that either "insider" term should not be used to discriminate or target individuals from one particular country of origin or background.

2. Clarity

There are several areas where more clarity could help institutions most efficiently meet the proposed requirements, beyond those mentioned above regarding the funding threshold.

APLU appreciates the definitional appendix. **OSTP should ensure continuity of definitions across NSPM-33, the NSPM-33 implementation memo, the Research Security Programs Standard Requirement, and future agency implementation guidance.** For instance, page 3 of the draft instructs institutions to maintain clear response procedures to address reports of "allegations of research security non-compliance" and that they must report "incidents of research security violations" to federal awarding agencies, while page 4 calls on institutions to provide tailored training to affected individuals related to a "research security breach finding." However, the appendix identifies only "research security incident" and "security incident." This mixing of terms could cause confusion, and clarity is needed on reporting and investigation responsibilities including to determine the veracity of any "allegation" before reporting it to a federal agency.

Additionally, institutions have expressed confusion regarding the foreign travel security section of the draft. The definition of "covered individual" does not comport with the definition included in "covered international travel" especially with regard to mentioning students in the covered international travel definition. This section also calls for institutions to maintain records without signifying the length of time these records must be maintained. It also calls for "A disclosure and authorization requirement in advance of international travel." The Standard Requirement should clarify if the covered individual should disclose and seek authorization from the federal agency or from the institution. There also seems to be a misalignment between the definitional terms "Covered International Travel" and "International travel." **Several APLU member institutions have also suggested OSTP should consider a more risk informed approach to the travel authorization and tracking section, including the possibility of tracking authorizations for only those countries considered at high risk for foreign interference.**

3. Feasibility

The Cybersecurity requirements are likely to be more difficult to implement and could be quite burdensome for some institutions**.** The requirements seem to be based on requirements for securing contractor information systems containing federal proprietary data and information. These requirements are not simple for universities to adopt quickly especially if institutions have diffuse IT systems across multiple schools and departments. In addition, university systems often contain data that is ultimately meant to be shared with the public and used by students, who more often than not are using their own computers to log on to university systems.

With regard to the Research Security Training requirements, it is helpful that the National Science Foundation (NSF) is funding work to create common training modules related to four of the attributes listed on page 4. **The Standard Requirement should clarify that the draft policy is not requiring institutions to provide nine specific training programs but that these topics can be incorporated into existing responsible conduct trainings or could be included in the common training modules NSF is helping to create. Additionally, the Standard Requirement should be clarified to limit research security training to covered personnel.** The reference to "new personnel" on page 4 has led some institutions to assume this means all new employees including those who have no duties related to research. Application to all institutional employees would be overly burdensome and inefficient.

4. Burden

Administrative burden is a concern for both universities and the federal government, and the generation or storage of unnecessary information adds to the cost of performing research. APLU appreciates COGR's recent Phase I cost study of institutions focused on the implementation of the disclosure requirements called for in NSPM-33. That study indicated costs of between ~$500,000 (large institutions) and $100,000 (small institutions). While we do not know of a full cost study on implementation of the Research Security Program, we have heard anecdotally from institutions that they may be facing over $1 million in costs in the first year of implementation. **OSTP should consider a phased approach or pilot for some of the requirements to help institutions better manage implementation costs.**

As a component of the OSTP draft research training requirements, universities are directed to "maintain the ability to certify that personnel have completed the required training for the purposes of Federal R&D award applications". **The Standard Requirement should clarify whether training certifications will be a required component of all grant award applications or will only be via federal agency request. Additionally, the requirements for certification should be made clear including basic required information, preservation time for university records, and the information specific to certification of tailored training completion for non-compliant PIs.**

5. Compliance.

APLU appreciates OSTP's proposal for self-certification; however, one year for compliance with all of the provisions may be difficult for some institutions. In addition, clarity is needed on the call for a publicly available status report 120 days from issuance of the regulation. **OSTP should provide information on the elements of a compliance status report.** OSTP's draft proposal calls for institutions to maintain a description of their finalized research security program, to make it public on their website, and to provide documentation to research agencies. **Compliance with these requirements would be much easier if there were suggested standards and reporting forms so as not to encourage federal agencies to make differing interpretations as to what constitutes compliance. In addition, further clarity on aspects of the research security plan that can be, or should be, withheld from public websites should be provided.** Public disclosure of certain aspects of cyber security and risk assessment could be counterproductive and provide competitors with a roadmap to circumvent security procedures.

On a final note, **APLU urges OSTP to clarify that compliance checks or enforcement will not be subject to individual agency issued standards for certification. Annual certification compliance should be based on a single set of interpretations that are shared across federal agencies.** As indicated in the draft Standard Requirement, some agencies may add security components necessary for classified or CUI research, but these should not be part of the base certification of a research security plan.

We again thank OSTP for the opportunity to comment and want to work with you to ensure the proper protection of federally funded research and development investments.

Sincerely

Mark Becker
President, Association of Public & Land-grant Universities