MEMORANDUM

TO: researchsecurity@ostp.eop.gov

FROM: Association of American Universities
Tobin Smith, toby_smith@aau.edu
Meredith Asbury, meredith.asbury@aau.edu

DATE: May 31, 2023

Re: Request for Information; NSPM 33 Research Security Programs Standard Requirement

On behalf of the Association of American Universities, which represents America's leading research universities, we submit comments in response to the request for information on the draft research security programs standard requirements.[1] We appreciate the National Science and Technology Council's (NSTC) and the Office of Science and Technology Policy's (OSTP) work to put together these draft standard requirements. We also recognize and applaud the significant efforts undertaken by OSTP and federal research, security, and intelligence agencies to coordinate efforts to harmonize and create uniform policies aimed at addressing and mitigating risks posed by adversarial foreign governments to federally funded research.

In addition to our comments, we also align ourselves and support comments submitted by the Council on Governmental Relations (COGR), the Association of Public and Land-grant Universities (APLU), the American Council on Education (ACE), the Association of American Medical Colleges (AAMC), the Association of University Export Control Officers (AUECO), and EDUCAUSE. We would also draw attention to comments we previously submitted with several other associations recommending OSTP conduct listening sessions to receive feedback on the proposed research security programs standard requirements from various higher education associations, scientific societies, university representatives, and other key stakeholders.[2]

We have organized our comments below to first address some key overarching points followed by comments specific to the four program requirements. As requested in the *Federal Register* notice, the requested topics are indicated throughout the comments.[3]

Overarching Considerations

Our member institutions take seriously the threats posed by malign foreign actors and the obligation of U.S. institutions of higher education to properly mitigate risks to federally funded research. AAU, along with APLU, has surveyed our members, and knows they have taken actions to address research security concerns ranging from increasing campuswide communication and coordination of research security efforts; enhancing their conflict-of-interest and conflict-of-commitment policies; increasing review and scrutiny of international collaborations, contracts, and foreign gifts; and enhanced communication and cooperation with the FBI and other security, law enforcement, and research agencies. Universities have

also been working to ensure compliance with new research security requirements including in previous National Defense Authorization Acts and the CHIPS and Science Act.

We appreciate the NSTC's and OSTP's efforts to engage the academic research community and stakeholders in the process to finalize the research security program standard requirements. We also appreciate that the drafted requirements provide flexibility to institutions to implement and meet certain requirements. However, we find that specific improvements would make the standards clearer and more effective.

Account for Risk-Based Standards [2, 3, 4, 5]

The NSPM-33 implementation guidance issued in January 2022 states that "agencies should incorporate measures that are risk-based, in the sense that they provide meaningful contributions to addressing identified risks to research security and integrity and offer tangible benefit that justifies any accompanying cost or burden."[4] The use of a risk-based approach to the development of research security program standard requirements is a concept that AAU strongly supports. Accounting for risk through factors such as the type of research being performed and/or where the research is taking place is vital to identifying and mitigating the most significant threats. We are concerned that the current draft requirements fail to fully take a risk-based approach regarding both the breadth and nature of the proposed measures.

The lack of a risk-based approach is particularly concerning related to the foreign travel security section of the draft research security program standard requirements. The NSPM-33 implementation guidance says that agencies should require research organizations to maintain travel policies for faculty and staff "that would put a person at risk." The lack of any differentiation between risk associated with different types of research and travel to specific high-risk countries versus low-risk countries will significantly burden institutions, regardless of their size, with the collection of unnecessary new information for nearly all faculty and staff conducting federally funded research, regardless of whether their work is considered low- or high-risk. The broad application of the travel reporting requirement will require universities to collect an ocean of data – so much data in fact that it will be difficult for universities to identify and put in place measures to effectively mitigate the most serious travel risks.

We ask that the final requirements provide institutions flexibility to take a risk-based approach to developing their research security program.

Clarify Definitions to Ensure Compliance [2, 3, 5]

We thank the NSTC and OSTP for including an appendix of definitions in the draft research security program standard. However, we are concerned that some of the newly introduced definitions are not aligned with existing definitions contained in the NSPM-33 implementation guidance or in the CHIPS and Science Act. The use of multiple similarly worded terms, which all have different definitions, will make compliance confusing and difficult, particularly concerning what a reportable finding would consist of and to whom that finding should be shared.

We recommend that the appendix of definitions contained in the final requirements be aligned with those contained in previous NSPM-33 guidance and other statutory definitions to help prevent unnecessary confusion and to ensure institutional compliance.

Provide Interagency Consistency [1, 2, 3, 4, 5]
The NSPM-33 implementation guidance calls for consistency across agencies to "provide strong and effective measures to protect research security and reinforce adherence to research responsibilities, transparency, and equity."[5] The draft standard requirements suggest that federal research agencies will communicate the requirements for research security programs to research organizations as part of their funding agreement processes. Given the guidance's and draft standards' commitment to maintaining consistency, we would hope that agency variation or duplication of certification requirements will only be permitted in very limited and distinct circumstances. Having each agency maintain its own certification processes for research security programs would complicate oversight, lead to duplicative and conflicting requirements, and burden institutions with multiple certification processes.

We ask that the final requirements clearly state one set of standards, the agency which will have compliance oversight, and the circumstances when specific research security program requirements by additional agencies will be permitted.

Clarify Implementation Timeline [2, 3, 5]
The draft standard requirements note that self-certification takes place "one year from the issuance of this Memorandum" and adds a new requirement for institutions to publicly post a status report 120 days after the "issuance of this Memorandum." It is unclear if these timelines begin based on OSTP's March 5 release date of the draft requirements or the release date of the final requirements or when agencies issue their own final requirements. Implementation of new requirements will take time and, therefore, it is vital to know when that clock begins and ends.

We ask that the final requirements provide clarity on the effective date of the final requirements and rescind the 120-day status report unless there is a clear reason why such a requirement is necessary.

Program Requirement Areas

Certification Requirements [2, 3, 5]
We appreciate that the standards provide some discretion and flexibility for institutions to meet the research security program certification requirements. Given the wide range of institution types that will need to comply with the standard requirements, there will be several ways to approach the structure, assessment, and monitoring of an institution's program that will also depend on an institution's staff and financial resources.

The final standards should recognize that a one-size-fits-all approach to implementation is not feasible and, therefore, should provide, to the greatest extent possible, flexibility for an institution to use its own discretion for the design and oversight of its program to uniquely meet the needs of the specific research environments that exist on its campus.

The "overarching program requirements and certification" section states that institutions must "report incidents of research security violations to the federal awarding agency or agencies."[6] Greater clarity is needed to identify what is considered a "reportable event." Additionally, the terms "research security incident," "national security incident," and "research security breach finding" are all similar to each other and make it difficult to distinguish whether they are speaking to different or same types of incidents.

We ask that the final requirements clarify what "reportable events" are and that the terms used to define those events or "incidents" are consistent.

Foreign Travel Security [2, 3, 4, 5]
Universities recognize that in a time of heightened global tensions, the collection of data on travel to certain countries can be a useful monitoring tool if targeted and focused on specific high-risk countries and aimed at mitigating specific concerns. We are concerned that as presented, however, the current foreign travel security program requirements are overly broad and not focused enough on addressing specific risks posed by travel to certain higher risk countries. As a result, the two drafted components of this section – disclosure and authorization – will create a significant new and unnecessary burden for institutions, with no clarity on what or how the broad-based collection of travel or authorization of travel to all foreign countries would address a stated risk or concern of a certain region, entity, and/or field of study.

Relatedly, the definitions for "covered individual," "covered international travel," and "international travel" create confusion on who and what needs to be reported. Consistent definitions and use of terms would help clarify who needs to report their travel and what travel is necessary to disclose. As drafted, it is unclear what exactly needs to be reported and what does not require reporting. If institutions must track all international travel related to research, regardless of whether the travel is relatively low risk based on both the nature of the research activity and the country being visited – for example, a faculty member travelling to Canada to give a presentation at a conference on bird migratory patterns – this will delay identification of and attention to the most serious risks. To be effective, concerns with foreign travel must be explicitly clear, specific, and risk based. *The final standard requirements should narrowly focus on the risks associated with specific research areas and travel to specific countries where the federal government is seeking to mitigate risk through collection of this information.*

In addition to this new, expansive, disclosure requirement, institutions would be required to *pre-approve* international travel for faculty and staff. This raises many questions including who would provide such approval, what does "approval" mean, what criteria need to be used, and how an institution would handle authorization of international travel already included in a federally awarded grant budget. *As institutions consider these questions, they should have the flexibility to determine the criteria for authorizing travel that would allow for federally approved budgets to be considered fully approved.*

Research Security Training [2, 4, 5]
We ask that the final requirements recognize that there are multiple ways institutions can satisfy the requirement to provide instruction on the nine identified areas, and that many of those topics have already been implemented through existing training programs which are regularly reviewed and updated. Additionally, as institutions await new NSF training modules on research security, it would be helpful to know how those training modules will satisfy the nine training areas mentioned in the draft requirements.

Given the multitude of training requirements, it is important for consistent definitions to be used that clearly identify who is required to receive training. *We ask that the standards be aligned with*

requirements of the CHIPS and Science Act, which statutorily defines a "covered individual." Multiple definitions of who should receive training will lead to unnecessary confusion and create challenges for our institutions as they seek to implement and comply with the new training requirements and ensure that the appropriate individuals receive the training. *Additionally, we ask that the training requirements consider an individual's research and responsibilities and that certain training elements may not be applicable or relevant to all researchers, particularly in areas of research work and other scholarly areas determined to be low risk.*

Cybersecurity [2, 3, 4, 5]
We recognize that OSTP's intention with the cybersecurity requirements is to provide clear guidelines for institutions to protect their information systems used to store, transmit, and conduct federally funded R&D. However, we feel that, as currently crafted, these protocols would complicate compliance and do not provide enough flexibility to institutions to implement safeguarding measures that are most appropriate to the research being conducted at individual institutions. The requirements outlined in the proposed guidance are similar to those intended to cover federal contractors, but do not fit well for the academic research environment. *Therefore, we ask that institutions be provided flexibility to determine which cybersecurity protocols are realistically achievable for their research environments.*

We support and refer to EDUCAUSE's comment letter, which provides a more detailed response to the concerns with the cybersecurity standard requirements for research universities.

Export Control Training [2, 3, 4, 5]
AAU member institutions have long had in place robust measures to provide relevant personnel information on conducting research subject to export control restrictions. The program requirements should recognize that a one-size-fits-all approach to export control training is not the best approach to ensure maximum results. Instead, such training should be targeted to certain faculty and students working in high-risk research areas. Research universities and their export control officers can best assess their research environment and where such training is most appropriate. *We urge some flexibility to enable universities to make such assessments as opposed to requiring blanket export control training for all faculty and students.*

We also ask that the example provided in the draft requirements be removed as it is inconsistent with the definition of fundamental research. Alternatively, it may be helpful to outline what the fundamental research exclusion (FRE) does allow that is not considered subject to export controls.

We support and draw reference to the Association of University Export Control Officers (AUECO) comment letter, which provides a more detailed response addressing the concerns with the export control training standard requirements for research universities.

Conclusion
In conclusion, we greatly appreciate the NSTC's and OSTP's collaborative work with federal research agencies to put together these draft standard requirements. We also recognize there is significant work ahead to ensure these program standards are as effective as possible, including ensuring there are consistently defined terms, a clear timeline for implementation, and clarity on risk and institutional flexibility. We look forward to working with you to finalize the requirements.

[1] "DRAFT Research Security Programs Standard Requirement," *Subcommittee on Research Security, National Science and Technology Council, Office of Science and Technology Policy*, February 2023

[2] "AAU Signs Letter Requesting Listening Sessions on Research Security Program Standards," April 13, 2023

[3] (1) Equity, (2) Clarity, (3) Feasibility, (4) Burden, and (5) Compliance

[4] "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development," *National Science and Technology Council Subcommittee on Research*, January 2022, page 1.

[5] Ibid. page ix.

[6] Ibid. page 3.