

Gloria Waters  
Vice President and Associate Provost for Research  
One Silber Way  
Boston, Massachusetts 02215  
T 617-358-2040 F 617-358-1940

June 5, 2023

Submitted via email to [researchsecurity@ostp.eop.gov](mailto:researchsecurity@ostp.eop.gov)

Subject: Comment on Research Security Programs

Boston University (BU) appreciates the opportunity to respond to the Request for Information on the NSPM 33 Research Security Programs Standard Requirement (Standards). BU is a private research university that competed for more than \$400 million in federal research funding in fiscal year 2022. We share the Administration's commitment to protecting both research security and openness, as well as ensuring that research security policies do not fuel xenophobia or prejudice.

BU is a member of and supports the comments submitted by the Association of American Universities (AAU) and the Council on Governmental Relations (COGR), among others. We also share our views below, organized along the themes you have requested.

## **2. Clarity**

- Interagency Consistency: BU echoes the comments of higher education and academic research associations that have expressed the need for one set of federal standards, with one agency providing compliance oversight. Multiple agency standards would create confusion for our researchers and potentially lead to unintended violations of differing agency policies. A single uniform federal standard would alleviate those tensions.
- Research Security Training: BU recommends greater clarity from OSTP on who would be subject to research security training to ensure a targeted, effective approach. Specifically, the Standards should align with the CHIPS and Science Act of 2022 definitions of who should be covered by research security training and what such training should entail.
- Foreign Travel Security: Clarity is needed on whether visiting certain locations or participating in certain activities will be prohibited (beyond existing export regulations, screenings, and embargoes). This would be best executed in coordination with existing federal export control regulations. Furthermore, the Standards should specify that institutions may develop their own disclosure and authorization requirements, making clear what factors institutions should address.

## **3. Feasibility**

- Foreign Travel Security: We recommend that the Standards apply only to foreign travel directly connected to a researcher's affiliation with their institution and with a federally funded research activity. As a university that engages in international research collaborations, employs international faculty and staff, and educates and trains students from across the globe, it is imperative to have a risk-based approach to foreign travel security that can be tailored to the specifics of the research being conducted, where, and by whom. A blanket foreign travel pre-registration requirement that is not tied to risk would be difficult to comply with and unlikely to improve research security.
- Cybersecurity: OSTP should consider replacing the list of cybersecurity protocols with a requirement for research cybersecurity plans that address key objectives and are risk-based to allow institutions to

match requirements and resources to actual needs. This would allow us to continuously improve our cybersecurity without unduly burdening research projects. Barring a shift to a risk-based approach, the requirements should instead allow institutional discretion in implementing cybersecurity protocols to maximize compliance success.

- Export Control Training: For these trainings, the Standards should provide institutions with the discretion to decide what information needs to be provided to best suit the needs of their research community. Additionally, BU concurs with our associations' statements that the example provided in the standards is inconsistent with the definition of fundamental research and should be removed from the final requirements. Furthermore, the standards should acknowledge the importance of the fundamental research exclusion and should consider outlining what is permitted under the exception rather than list what activities are prohibited.

#### **4. Burden**

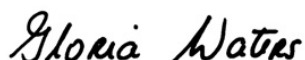
- Account for Risk-Based Standards: BU strongly recommends the use of risk-based standards for the implementation of a research security program. Blanket standards with no risk-based distinctions in their applicability or requirements – such as the type of research being conducted, where it is being conducted, and by whom – will likely result in increased barriers to vital international academic and research collaborations and potential bias or xenophobia depending on the country of origin of our students and faculty members.

#### **5. Compliance**

- Research Security Training: The Standards should provide compliance flexibility for research institutions. Allowing us to integrate existing training modules, determine the best method for training, and establish our own compliance tracking system will expedite our ability to comply.
- Self-Certification: We agree that self-certification is appropriate as the primary model of compliance. OSTP should afford maximum flexibility to institutions in structuring, assessing, and monitoring their programs, and allow us to leverage our existing programs and activities to fulfill the requirements. This flexibility is typically afforded to institutions in their implementation of most federal regulations and would be beneficial. A standard certification statement for institutions to sign or specific requirements for an institution's certification statement should be provided. Additionally, clarification is needed on the method and frequency of certification.

Thank you again for this opportunity to comment. We look forward to continuing to work with OSTP to implement research security standards that maintain the integrity of our federal research enterprise and ensure that the U.S. remains the global leader in science and innovation.

Sincerely,



Gloria Waters  
Vice President and Associate Provost for Research