NSPM-33 Research Security Program Standard Requirement Comments

Key Messages

This document was created in collaboration with a group of higher education associations to outline some of the key topics and messages we have discussed which may also help inform an institution's response to the Request for Information (RFI) from the White House Office of Science and Technology Policy (OSTP) related to the proposed requirements for an institutional research security program, with a response deadline of June 5, 2023. Each association or organization will submit its own comments in response to the RFI that may differ in wording and focus from the considerations below.

Topline Messages

Account for Risk-Based Standards

- For the final research security program standards ("Standards") to be considered effective, they must be based on levels of risk that account for factors including the type of research being performed and where the research is taking place. The lack of a risk-based approach is particularly concerning related to the foreign travel security section of the draft research security program standards. The lack of a risk-based approach will add significant burden to institutions with unnecessary new information collection which is also not helpful to mitigating risks.

Clarify Definitions to Ensure Compliance

- We thank the NSTC and OSTP for including an appendix of definitions in the draft Standards. However, we are concerned that the defined terms are inconsistent with those defined elsewhere in NSPM-33 and in the NSPM-33 implementation guidance.
- In other cases, defined terms from the appendix are not used in the Standards. Compliance will suffer if there are inconsistent definitions and similarly if certain terms in the Standards are not defined or aligned with existing definitions in NSPM-33 and the CHIPS and Science Act.

Provide Interagency Consistency

- It is unclear which agency (or agencies) will have compliance oversight of these new Standards. We ask that it be made abundantly clear in the final Standards that there is one set of OSTP-issued standards to which institutions must certify and comply overseen by one single agency. Agency variation on certification will complicate oversight, lead to duplicative and conflicting requirements, burden institutions with multiple certification processes, and confuse faculty researchers.
- Any additional agency-specific requirements should be permitted only in limited circumstances that are clearly delineated in the standards, e.g., proposals that involve CUI, export controlled, proprietary, or classified information.

Clarify Implementation Timeline

- The requirements state 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." The draft final research security program standard requirements must clearly state the effective date of the final requirements. We also ask that the 120 day "status report" be rescinded unless there's a clear reason as to why such a requirement is necessary.

Appreciation for Comment Process and Flexibilities

- We appreciate NSTC 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 Standards provide flexibility to institutions in determining how they will meet certain requirements and self-certify as to the implementation of their program.

Messages Specific to Standard Requirement Areas

Covered Research Organizations

- **One Source for Calculating Triggering Financial Threshold**: For clarity, the Standards should state that USASpending.gov is the single source for calculating the financial threshold that triggers the research security program requirement and identify the specific USASpending.gov profile/profile items to be used for the calculation.
- **Agency Notice of Applicability**: To reduce institutional burden, OSTP (or an alternative single federal agency) should maintain a non-public record of institutions who meet the financial threshold and annually provide each institution on that list with notice as to whether the financial threshold is met, along with a description of the process to be following if the institution believes the calculation is in error. Additionally, if an institution reaches the financial threshold in a subsequent year, it should be clear when they must begin to comply with the requirements and the deadline to which they must certify they have a program in place. Alternatively, institutions whose research portfolios fall below the financial threshold should not be penalized in agency funding decisions if they aren't required to have a research security program in place.

Overarching Program Requirements and Certification

- **Detail Minimum Standards for Documentation**: The Standard should provide minimum requirements for the required research security program description and documentation, along with the text of the certification statement that institutions will be required to execute.
- **Ensure Institutional Flexibility in Implementation**: OSTP should afford maximum flexibility to institutions in structuring, assessing, and monitoring their programs, and allow them to leverage existing programs and activities to fulfill requirements. To avoid security compromises, the Standards should make clear that only a high-level program description must be publicly posted.
- **Clear Definition of Reportable Events**: The proposed Standards use multiple terms for reportable events (e.g., research security incident, security incident, incident of research security violation, research security breach), and not all of these terms are defined. The Standards should ensure that any reportable event is signified by a clearly defined term that

unambiguously informs institutions of what must be reported to whom and when the report is to be made.

- **Cognizance of Other Regulatory Reporting Requirements**: The Standards must account for the potential of overlapping regulatory-specific reporting requirements. In cases where such standards penalize the use of other reporting mechanisms (including reporting under the Standards), institutions must be permitted to report via regulatory-specific channels. Additionally, the Standards should clearly state that their reporting requirements will not in cases in which an institution utilizes existing voluntary disclosure processes (e.g., voluntary disclosure in the area of export controls).

Foreign Travel Security Section

- **Risk-Based**: As noted, it is imperative that these standards be risk-based, with controls tailored to the risks presented by the location of the travel and the type and circumstances of the research activities.
- **Clarify Definitions**: The definitions for 'covered individual,' 'covered international travel,' and 'international travel' must be streamlined to avoid confusion about what travel is subject to the requirements. It is imperative that one definition specifies who needs to report and what travel is necessary to disclose.
- **Confine to Travel that has a Nexus to the Institution and Federally Funded Research**: The Standards should only cover travel that has a nexus to the institution and to federally funded research activities. At a minimum, the definition of Covered International Travel should be revised to encompass only Covered Individuals' official institutional business travel that contributes in a substantive, meaningful way to the Covered Individual's federally funded R&D project.
- **Disclosure/Authorization Criteria:** The Standards should make clear that institutions have the flexibility to establish disclosure and authorization requirements, and they should identify any factors that OSTP believes are relevant in developing such criteria.

Research Security Training Section

- **Clarify Definition and Flexibilities**: The definition of 'covered individual' should be employed in this section to identify who is to receive research security training. The Standards must also recognize there are multiple ways for institutions to satisfy the requirement, including alignment of existing training requirements with what the Standards outline. For example, cybersecurity training is typically handled separately from research security training. The training Standards should afford sufficient flexibility to institutions with respect to how, when, and where they address the training topics so long as the topics themselves are fully covered. The Standards should also make clear that Institutions have the flexibility to determine how they will track the completion of any required training.
- **NSF Training Modules**: The Standards should clearly outline how the four NSF training modules that are currently under development will satisfy the nine training requirements, and compliance effective dates should be aligned with the date(s) on which the modules will be made available.
- **Risk-Based**: The Standards are monolithic and apply without regard to a researcher's individual circumstances/responsibilities or the nature/circumstances of their research. To address this

issue, the Standards should be aligned with the requirements of the CHIPS and Science Act of 2022, including the Act's definition of "Covered Individual," and training content should be limited to risks of malign foreign talent recruitment programs and/or insider threats. The training audience should be similarly limited to researchers who conduct research that may be subject to such threats.

Cybersecurity Section

- **Shift from Protocol List to Risk Management:** Replacing the list of cybersecurity protocols with a requirement for research cybersecurity plans that address key objectives and are risk-based would allow institutions to match requirements and resources to actual needs, facilitating continuous improvement in cybersecurity without unduly burdening research projects.
- **Recognize the Need for Institutional Discretion:** Barring a shift to a risk-based approach, institutions will have to exercise discretion through institutional policy, as documented in their research security programs, to make compliance with the cybersecurity protocols realistically achievable. The research security program requirements should clearly allow for such discretion.
- **Allow for Alternative Measures:** Given the diversity of institutional/research contexts, all of the cybersecurity protocols will not work in all cases without creating undue burdens—and in some situations, one or more may not work at all. Institutions must be able to apply effective alternatives when needed, again noting that such cases must be appropriately documented.
- **Allow for Plans of Action and Milestones (POAMs):** Institutions striving in good faith to fulfill the protocols, and particularly those that have historically faced resource challenges, should have an avenue for addressing compliance even if all measures are not fully in place by the relevant deadline. The Department of Defense (DoD) approach of using POAMs to bridge compliance requirements with capabilities may serve as an effective model in this context, too.

Export Control Training Section

- **Institutional Discretion**: The Standards should recognize that a one-size-fits-all approach is not the goal of this training requirement. Institutions can best assess the needs of their research community and should be provided with the discretion to determine what is important to share and to train on specific to their research environment.
- **Remove Provided Example**: The example provided in the Standards is inconsistent with the definition of fundamental research and should be removed from the final requirements.
- **Limits to the Fundamental Research Exclusion**: The Standards should recognize the importance of the fundamental research exclusion (FRE) and rather than outline explicit limitations, it may be more instructive to outline what the FRE does allow that is not subject to export controls.

Other Information

Federal Register Notice
https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement

Draft Research Security Program Standard Requirement

https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

Notes on Formatting from Federal Register Notice

- Submissions must not exceed 5 pages (exclusive of cover page) in 12-point or larger font, with a page number provided on each page.
- Responses should include the name of the person(s) or organization(s) filing the comment, as well as the respondent type (*e.g.,* academic institution, advocacy group, professional society, community-based organization, industry, member of the public, government, other).
- A list of references does not count toward the 5-page limit.
- Respondents are asked to note the corresponding number/s to which their responses pertain:
    1. Equity
    2. Clarity
    3. Feasibility
    4. Burden
    5. Compliance