[3270-F1]

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Request for Information; NSPM 33 Research Security Programs Standard Requirement

AGENCY: Office of Science and Technology Policy (OSTP).

ACTION: Notice and request for comments.

SUMMARY: The Office of Science and Technology Policy (OSTP) requests comments from the public on draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). The draft Standard Requirement has been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementing this requirement.

DATES: Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023.

ADDRESSES: Submit comments electronically to researchsecurity@ostp.eop.gov with the subject line <<*Comment on Research Security Programs*>> by the deadline. Due to time constraints, mailed paper submissions will not be accepted.

Instructions: Response to this notice is voluntary. Responses to this notice may be used by the government for program planning on a non-attribution basis. OSTP therefore requests that no business proprietary information or copyrighted information be submitted in response to this notice. Please note that the U.S. Government will not pay for response preparation, or for the use of any information contained in the response.

Responses may address one or as many topics as desired from the enumerated list provided in this request for comment, noting the corresponding number of the topic(s) to which the response pertains. 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). Respondent's role in the organization may also be provided (*e.g.,* researcher, administrator, student, program manager, journalist) on a voluntary basis.

Please also organize your responses such that substantive comments are at the beginning of the document and more procedural and/or technical comments are at the end. This format will help us to absorb and respond to your comments in a more organized way.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials; these materials, as well as a list of references, do not count toward the 5-page limit. No business proprietary information, copyrighted information, or personally identifiable information (aside from that requested above) should be submitted in response to this request for comment. Comments submitted in response to this notice are subject to the Freedom of Information Act. Comments submitted may be posted online or otherwise released publicly.

FOR FURTHER INFORMATION CONTACT: Direct questions to Kei Koizumi at researchsecurity@ostp.eop.gov; tel: 202-456-4444.

SUPPLEMENTARY INFORMATION: National Security Presidential Memorandum 33 provides for a National Security Strategy for United States Government-Supported Research and Development. Section 4(g) directs that, "heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training."

On January 4, 2022, the OSTP's National Science and Technology Council released Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33). NSPM-33 charges OSTP with "coordina[ting] activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks." A similar charge is captured in the National Defense Authorization Act of 2020.[1]

The resulting Guidance, called for by the Director of OSTP, delivers on three key priorities, consistent with the values of the Biden-Harris Administration: (1) protecting America's security AND openness; (2) being clear in our delivery of guidance and information to impacted communities, so that compliance with NSPM-33 is easy, straightforward, and minimally burdensome; and (3) ensuring that our policies do not fuel xenophobia or prejudice.

The Guidance also captured next steps regarding the implementation of a Standard Requirement for Research Security Programs (hereinafter shortened to 'Standard Requirement'), stating on page 19:

"OSTP, in consultation with the NSTC Subcommittee on Research Security, OMB, and external stakeholders, will develop a standardized requirement for uniform implementation across research agencies. Following a 90-day external engagement period, OSTP will complete the standardized requirement in the subsequent 120 days, and, upon completion, work with OMB to develop a plan to implement the standardized requirement. Upon receipt of the standards, relevant research agencies should engage with external stakeholders to ensure that program

[1] The language from the 2020 NDAA (Public Law 116-92), captured in Sec. 1746. (a), states: "In general.--The Director of the Office of Science and Technology Policy, acting through the National Science and Technology Council, in consultation with the National Security Advisor, shall establish or designate an interagency working group to coordinate activities to protect federally funded research and development from foreign interference, cyber attacks, theft, or espionage and to develop common definitions and best practices for Federal science agencies and grantees, while accounting for the importance of the open exchange of ideas and international talent required for scientific progression and American leadership in science and technology."

requirements are appropriate to the broad range of organizations that are subject to the requirement."

In fulfillment of this statement, a draft Standard Requirement has been completed and is available for review at: https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf.

To enable further coordination, OSTP is leading engagement with external stakeholders, as the Guidance described. This request for comment is an important source of engagement and is meant to give the public an opportunity to review and provide feedback on the draft Standard Requirement. Through this request for comment, OSTP seeks public input on the Standard Requirement, with special attention to equity, clarity, feasibility, burden, and compliance.

Scope: OSTP invites comment from any interested stakeholders. In particular, OSTP is interested in input from research organizations that will be subject to the Research Security Program requirement, researchers within those organizations, professional organizations representing those organizations, and organizations representing diverse interests across the U.S. research ecosystem.

Information Requested: Respondents may provide information for one or more of the topics included below. Respondents are asked to note the corresponding number/s to which responses pertain.

1. **Equity.** The NSPM-33 implementation Guidance requires that research security policies and practices are implemented in an equitable and non-discriminatory fashion. Are there any areas of the Standard Requirement that have not, in your view, upheld the fundamental commitments to equity and non-discrimination?
2. **Clarity.** It is essential that the Research Security Programs Standard Requirement is clear. Clarity enables equity, transparency, and compliance. Comments on clarity throughout the Standard Requirement are especially appreciated, particularly as they pertain to the ability of organizations to understand and meet the provisions of the

Standard Requirement. Your perspectives on the extent to which the Standard Requirement is clear and allows for straightforward adoption are of great interest.

3. **Feasibility.** The Research Security Program Standard Requirement will be most successful if covered organizations view adoption as feasible. With that in mind, are there aspects of the Standard Requirement that are concerning in terms of implementation? If so, how and why?
4. **Burden**. Closely related to feasibility is burden. Engagement with the research community has allowed us to understand that concerns about burden, whether in regard to financial or administrative burden, are high. Provisions in the Standard Requirement have been scoped with an aim to lessen burden, such as centralized certification on SAM.gov and technical assistance for development of research security training. Are there other measures that would help to lower the burden on the research community in implementing the Standard Requirement?
5. **Compliance**. The draft Standard Requirement suggests self-certification as the primary model of compliance with the requirements, with initially certification required one year after the issuance of the Standard Requirement. What are your perspectives on these approaches? Are there others that should be considered?

Dated: March 2, 2023.

Stacy Murphy,

Deputy Chief Operations Officer/Security Officer.

[FR Doc. 2023-04660 Filed: 3/6/2023 8:45 am; Publication Date: 3/7/2023]