COGR

An Association of Research Institutions

May 30, 2023

Submitted via email to researchsecurity@ostp.eop.gov
Office of Science & Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Ave.
Washington, D.C. 20504

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

To Whom It May Concern:

COGR is an association of over 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. COGR and its member institutions recognize the importance of ensuring research integrity and responding to malign foreign influence on federally funded research. Our institutions have worked, at significant time and cost,[1] to develop and promote effective practices in this area,[2] while fostering international collaborations that are vital to the success of the U.S. and global scientific enterprise. We appreciate the opportunity to comment on OSTP's proposed Research Security Program Standard Requirements ("Standards"), which will significantly impact institutions' procedures, processes, and training.

Key Goals that Must be Achieved to Ensure Standards' Success: ***The successful implementation of the Standards and the overall federal research security framework depends on whether the Standards are: (a) targeted in a risk-based manner, (b) consistent across all agencies, and (c) clearly delineated.*** Failure to accomplish these objectives will impede implementation, negatively affect results, and unnecessarily add to the already significant and unrecouped costs institutions are incurring to comply with research security and other compliance mandates.[3] Thus, COGR urges OSTP to take the following overarching steps with respect to the formulation/promulgation of the Standards:

- **Risk-Based**: Ensure that Standards are tailored to address the level of risk presented by the type and circumstances of the research and other activities they regulate. The NSPM-33 Implementation Guidance states that security measures are to be "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] and NSF's recently released JASON report[5] also supports this risk-based approach. Despite these calls for risk-based solutions, the travel, cyber, and research security training standards draw no risk-based distinctions in their applicability or requirements. Treating all researchers and research equally does not make the standards equitable; rather, an approach that is agnostic to research risk imposes unnecessary costs and burdens on low-risk research for which more stringent controls are unnecessary and counterproductive.

- **Consistency**: Ensure that federal agencies implement only one set of Standards to which institutions must certify compliance and that agencies include any additional security requirements in the Request for Proposal (RFP) only when there is an identified, substantive justification for the requirement that has been formally recognized by OSTP (e.g., presence of CUI). Agency promulgation of multiple standards is contrary to the Implementation Guidance and complicates training, causes confusion among researchers, and confounds compliance efforts.

- **Clarity**: Ensure that the Standards' Appendix contains a comprehensive set of clearly defined terms that are consistently used throughout the document. Further, these definitions should completely align with definitions of the same terms used in NSPM-33 and the Implementation Guidance.

Support for Other Comments: COGR and its partner higher education and academic research associations have consistently provided extensive input on proposed requirements in the research security arena.[6] Given the page limit on comments, COGR refers to and fully supports the following associations' responses: American Council on Education (ACE), Association of American Medical Colleges (AAMC), Association of American Universities (AAU), Association of Public and Land Grant Institutions (APLU), Association of University Export Control Officers (AUECO) and EDUCAUSE. Each response includes comments on provisions in the Standards for which the authoring association has specific knowledge/expertise. We especially support these associations' comments concerning cybersecurity and export controls, areas for which COGR hasn't included specific comments.

COGR's Specific Comments: Our comments regarding specific Standard provisions are noted below. Per the Federal Register notice, each comment references one or more of the following topic numbers to which the comment pertains: (1) Equity, (2) Clarity, (3) Feasibility, (4) Burden, and (5) Compliance.

Introduction Section [2, 3, 4, 5]: This section should clearly state that the Standards "memorandum" issued by OSTP will contain the final research security program standards that all federal agencies will implement and to which institutions will be required to self-certify. The current Standards ambiguously state that the "Memorandum provides further details on appropriate standards"[7] and that "Federal research agencies may impose additional requirements beyond these standards."[8] The Standards should make clear that additional agency requirements are not part of the research security program standards, but rather will be included in a solicitation only when there is an identified, OSTP-approved justification. Further, this section should delineate the circumstances that justify additional agency requirements such as the presence in the project of CUI, proprietary information, or export-controlled technology. Permitting each agency to develop its own standards undercuts the Implementation Guidance's call for interagency consistency and impairs institutions' ability to implement robust compliance systems and processes.

Covered Research Organizations Section

- Definition and Calculation of Federal Science and Engineering Support [2, 3, 4]: The Standards place the burden of calculating the triggering financial threshold entirely on institutions. Further, they reference multiple sources (e.g., institutional financial records, specified NSF data) of financial data, as opposed to the Implementation Guidance's sole reliance on "spending recorded in USASpending.gov."[9] COGR urges OSTP to retain the

clarity of the single USAspending.gov source for calculating the threshold, and to identify the specific site profile and profile items to be used in the calculation. To improve feasibility and reduce institutional burden, COGR also strongly recommends that the Standards be amended to require a single entity such as OSTP to annually provide each institution with notice as to whether the institution meets the financial threshold, along with a process for disputing the agency's assessment if an institution believes the analysis is erroneous.

- Effective Date of Standards and Status Report Requirement [1, 2, 3, 4, 5]: The Implementation Guidance provides institutions with one year from the issuance of the formal requirements to comply. The Standards, however, call for self-certification of compliance "one year from the issuance of this Memorandum," and include a new requirement for public posting of an undefined "status report" 120 days after "issuance of this Memorandum." It is unclear whether the clock starts when OSTP issues a final Standards memorandum to agencies, or when each agency issues its own final standards. Again, COGR urges OSTP to unequivocally state that there is one set of research security program standards applied by all federal research funding agencies to which institutions must certify, and that all periods run from the date on which those single Standards are issued by OSTP in final form. Further, we question the usefulness of requiring a progress report after only 120 days of a 365-day implementation period has elapsed and recommend deletion of this directive. As institutions' experience with the NSPM-33 disclosure standards has demonstrated,[10] implementation will require costly, time-consuming changes to policies, processes, procedures, and information technology (IT) systems that will be extremely challenging to implement in one year, let alone make noteworthy progress in 120 days, particularly for smaller research institutions.

Overarching Program Requirements and Certification Section

- Certification Statement [1, 2]: The Standards should include the certification statement language so that institutions can ensure their implementation efforts will satisfy its requirements. Additionally, the Standards should make clear that institutions will be required to provide a single, annual certification of compliance with the final OSTP-issued research security program standards, not individual agency-issued standards.

- Written Supporting Materials [2, 3, 4]: The Standards should clearly describe any minimum requirements for the "description" of the institution's finalized research security program, and associated program "documentation," while affording maximum flexibility to institutions as to how best to structure such documentation (e.g., outline of how Standards are met, references to pertinent policies and procedures, etc.). Further, the Standards should state that only a high-level description of an institution's program must be posted on a publicly available website so as not to compromise institutional security protocols.

- Reportable Events [2, 3]: The Standards use multiple terms for reportable events including "research security incident," "security incident," "incident of research security violation," and "research security breach," yet only "research security incident" and "security incident" are defined in the Appendix. Further, these defined terms do not align with terms used in the text,[11] and their definitions fail to provide an adequate description of what must be reported.[12] Any reportable event should be signified by a defined term and that definition should be unambiguous and used consistently. Further, in cases where the Standards'

reporting requirements overlap or conflict with those of a federal agency (e.g., voluntary disclosure of an export controls violation), institutions must be expressly afforded the discretion to solely follow agency-specific reporting requirements without penalty.

- Program Management, Monitoring and Assessment [2, 3, 4]: The Implementation Guidance states that "[r]esearch organizations should be provided flexibility to structure the organization's research security program to best serve its particular needs, and to leverage existing programs and activities where relevant." This statement stands in opposition to the Standards' directive to "manage the required elements as an integrated program." Flexibility is the key to feasibility; thus, the integrated program mandate should be deleted.

Foreign Travel Security Section

- Scope of Covered Travel [2, 3, 4]: The Implementation Guidance states that travel requirements are to be implemented "as appropriate," but the Standards cover *all* international travel irrespective of the risk posed by travel location and/or research with which the travel is associated. COGR urges OSTP to reevaluate this section and revise it to apply travel security requirements only when the research in question and the travel destination present a security risk. At a minimum, OSTP should revise the definition of "Covered International Travel" to encompass only official institutional business travel by "Covered Individuals" that contributes in a substantive, meaningful way to the execution of the Covered Individual's federally funded research and development (R&D) project, and then employ the defined term in this section. As it stands, this section presents institutions with the untenable and costly task of overseeing large numbers of trips that may have no nexus with federal R&D and/or institutional responsibilities[13] and/or pose no security risks.

- Disclosure and Authorization Criteria [2, 3]: The Standards mandate a "disclosure and authorization requirement"[14] and should be amended to make clear that institutions have the authority to establish their own disclosure/authorization criteria, including the discretion to consider any international travel included in an awarded grant's budget as "authorized." If OSTP will not afford institutions this discretion, then the Standards should clearly delineate disclosure/authorization criteria.

Research Security Training Section

- Training Timing and Certification Requirements and Relationship to NSF-Produced Training Modules [2, 3, 4]: RECR and other existing training programs into which these requirements are to be incorporated[15] have widely varying training schedules. Additionally, the meaning of the term "orientation" as used in this section is unclear (e.g., new employee orientation, orientation to a research project). Accordingly, the Standards should be modified to clearly identify when initial and refresher training is required. Similarly, the Standards should state that certification regarding training is incorporated into the overarching certification, and if not, when/how institutions will certify. Finally, the Standards should explain how the NSF-developed training modules will satisfy training requirements (including training "update" requirements), and any training associated deadlines should run from the date the modules are available.

- Alignment with CHIPS and Science Act ("Act") [2, 3, 4]: At present, the Standards are monolithic and apply without regard to the individual circumstances/responsibilities of

trainees and the research they conduct. To correct this problem, the Standards should be aligned with the Act's requirements, including its scope, content, and definitions. In particular, the training audience should be consistent with the Act's definition of "Covered Individual" at §10638(1) and content requirements should be limited to training on the risks of "malign foreign talent recruitment programs" in accordance with §10632(f) of the Act and "insider threat awareness"[16] for individuals who conduct research that may be subject to such threats (e.g., CUI, proprietary information, export controlled).

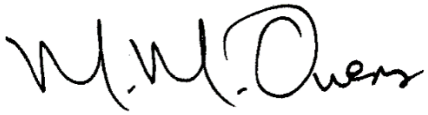
Definitional Appendix [2,3]: In addition to comments above regarding defined terms, we recommend that OSTP make the definitional changes described below to improve the clarity and feasibility of the Standards:

- Conflict of Commitment: Clarify that the word "improperly" modifies both "sharing" and "withholding."
- Controlled Unclassified Information (CUI): Conform this definition to that which appears on the referenced website, i.e., "Information that requires safeguarding or dissemination controls pursuant to and consistent with law, Federal regulations, and Government-wide policies."
- Foreign Government-Sponsored Talent Recruitment Programs: This term should be deleted and replaced by the term "Malign Foreign Talents Programs" as defined in §10638(4) of the Act.
- Gift: Conform the definition of this term to that set forth in the Implementation Guidance.
- Insider Threat: Conform the definition of this term to that set forth in the Implementation Guidance, which is limited to threats that affect the organization.

Conclusion: Finally, we note the striking absence of any Standards that describe in a positive fashion how international collaborations (including collaborations with China) can be carried out for fundamental, non-export controlled research that involves no proprietary or confidential information. This type of research often constitutes the bulk of research activity carried out by many institutions, and scientific collaborations in these areas across networks of researchers in all nations are crucial to maintaining U.S. scientific advantages. We encourage OSTP to include in the Standards the hallmarks and examples of such positive, permitted collaborations, and if collaboration with a particular country(ies) is considered too risky, OSTP should clearly state so.

We appreciate the opportunity to offer comments. Please direct any questions about this response to Kristin West, Director, Research Ethics and Compliance at kwest@cogr.edu or Robert Hardy, Director, Research Security & Intellectual Property at rhardy@cogr.edu.

Sincerely,



Matt Owens
President

[1] *See,* COGR, Research Security and the Cost of Compliance – Phase I Report, Disclosure Requirements (Nov. 2022) ("COGR Cost Report").
[2] *See, generally*, COGR Science and Security webpage.
[3] *Supra* n. 1.
[4] National Science & Technology Council, NSPM-33 Implementation Guidance ("Implementation Guidance")(Jan. 2022) at p. 1.
[5] JASON, Research Program on Research Security (Mar. 2023) at p. 22-23.
[6] *See,* COGR Science and Security webpage, Comment Letters.
[7] Standards at p. 2.
[8] *Id.*
[9] Implementation Guidance at p. 19.
[10] COGR Cost Report, *supra* n. 1. For additional examples of unfunded costs to institutions associated with large-scale regulatory change see COGR, Data Management & Sharing (DMS) and the Cost of Compliance: Results from the COGR Survey on the Cost of Complying with the New NIH DMS Policy (May 11, 2023).
[11] *See, e.g.,* Overarching Program Requirement Section requires reporting of undefined term "incidents of research security violations," which is inconsistent with defined terms "research security incident" and "security incident." Research Security Training Section requires reporting of undefined term "research security breach."
[12] *See, e.g.,* the vague bold italicized terms used in the following definitions: (a) Research Security Incident – "an ***action*** regarding Federal science and engineering support . . . ***due to improper influence***"; (b) Security Incident – "a range of ***possible*** actions, inactions, or events" that cause one or more of a broad range of listed results including items that institutions are incapable of ascertaining such as those which "[p]ose threats to national security interests and/or Federal Government" and "[h]ave a significant effect on the agency's safeguards and security program's capability to protect its interests."
[13] For example, sponsored travel for professional purposes that has no connection with federally funded research or institutional responsibilities that a 9-month faculty member undertakes during the summer term.
[14] Standards at p. 3.
[15] *Id.* at p. 4.
[16] Implementation Guidance at p. 18.