UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

OFFICE OF THE VICE PRESIDENT – RESEARCH AND INNOVATION

OFFICE OF THE PRESIDENT
1111 Franklin Street, 11th Floor
Oakland, California 94607-5200

June 5, 2023

Stacy Murphy
Deputy Chief Operations Officer/Security Officer
Submitted via email to researchsecurity@ostp.eop.gov

RE: RFI; NSPM 33 Research Security Program Standard Requirement (88 FR 14187)

Dear Ms. Murphy:

On behalf of the University of California system (UC)—comprised of ten campuses, six academic health centers, and three affiliated U.S. Department of Energy national laboratories—I write to respond to the Office of Science and Technology Policy's (OSTP) Request for Information (RFI) on the proposed Research Security Program Standard Requirements ("Standards") published in the *Federal Register* on March 7, 2023.

UC fully supports the overarching goal of the Standards and shares the government's goal of increasing the security profile of our research enterprise. However, without increased funding to accomplish this substantial task, implementation and compliance is not feasible. Like most research universities, UC is a nonprofit organization that does not accrue proceeds from federally-supported work. Therefore, we urge the federal government to fund implementation of the Standards, as suggested in our enclosed comments.

Thank you for the opportunity to provide our input.[1] If you have any questions concerning these comments, please contact Melissa Waver, Contracts and Grants Operations Officer, at Melissa.Waver@ucop.edu.

Sincerely,

Deborah Motton, Ph.D.
Executive Director
Research Policy Analysis & Coordination
(510) 587-6053
Deborah.Motton@ucop.edu

[1] In addition to our comments, UC endorses and concurs with the comments submitted by the following associations: Council on Governmental Relations (COGR), 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.

Before commenting on the specific contents of the draft Standards, UC would like to implore the federal government to adequately fund the government's mandate of increased research security. To accomplish this, we strongly encourage the Office of Management and Budget to raise or eliminate the 26% cap on administration costs charged to federal awards so that research institutions may recover research security costs as indirect costs. Alternatively, federal funding agencies should allow institutions to directly charge the costs of research security to federal awards. (See *Grants Management: Observations on Challenges with Access, Use, and Oversight* (GAO-23-106797), finding that "[a] lack of capacity for grant recipients can adversely affect their ability to successfully access, manage, and implement grant programs" and that "Federal agencies can help organizations mitigate capacity limitations . . . by making available federal or other revenue dedicated to covering the cost of grant administration and oversight.") Moreover, award budgets should be increased to account for these additional costs and to enable research organizations to continue contributing to U.S. economic and scientific competitiveness.

Introduction

UC concurs with and reiterates COGR's comments regarding the need to ensure the Standards apply to research based on risk. A constructive step in that direction would be to more accurately and narrowly define "R&D."

As noted in the Standards, "NSPM-33 charges OSTP with 'coordina[ting] activities to *protect Federally funded R&D* from foreign government interference." (Emphasis added.) NSPM-33 Section 1 further explains its purpose as protecting "*United States Government-supported* Research and Development (R&D)" because such R&D is "a key contributor to American *science and technology (S&T) innovation*." (Emphasis added.) Accordingly, NSPM-33 Section 4(g) makes the Standards applicable only to "research institutions receiving *Federal science and engineering support* in excess of 50 million dollars per year." (Emphasis added.)

Yet, the Standards do not clearly state that they apply only to federally-funded science and technology R&D programs. Instead, the current draft subjects a wide range of scholastic work to uniform security measures. For example, a federally-funded museum curation project would be required to have many of the same security protocols as a semiconductor research project.

To increase clarity, reduce burden, and heighten the feasibility of complying with the Standards, the definition of R&D should be changed as follows to add the underlined words:

> "Research and development (R&D) – "Includes basic research, applied research, and experimental development in the subject areas of natural science and engineering. . . ."

Additionally, for clarity, the term "federally-funded R&D" should replace the term "Federal science and engineering support" throughout the document, as the latter term would not be needed if R&D is redefined as noted above.

Covered Research Organizations

Rather than allowing only one year to implement the Standards, UC requests that OSTP give covered research institutions at least two years. Implementing the Standards in their entirety will

likely take longer than one year, especially for institutions that do not already have significant research administration infrastructure and resources. Fully implementing the standards will require recruiting and training staff to carry out the functions of organizations' research security programs, developing additional IT security resources, revising or creating institutional policies, creating compliant training programs, etc. Covered research organizations cannot feasibly accomplish all of this and have fully operational security programs within a 12-month period.

Additionally, the language regarding how much time organizations have to implement the Standards is ambiguous. The draft states that organizations "will have one year from the date of this Memorandum," but it is unclear which "memorandum" this refers to—the draft Standards or the final version. UC suggests changing this wording to clearly state that organizations will have at least two years from the date that the final Standards are published in the Federal Register.

Overarching Program Requirements and Certification

The language describing covered research organizations' responsibilities to share their research security program is unnecessarily burdensome and differs in significant ways from the requirement expressed in the NSPM-33 Implementation Guidance. The current draft language requires that covered research organizations 1) post a description of their research security programs on publicly-accessible websites and 2) provide documentation of "the maintained" program within 30 days of a request from a federal agency. Maintaining a website and separately providing the information on that website to individual agencies upon request is duplicative and inefficient. Either maintaining a website with the research security program information or providing it upon request would suffice to make research security programs transparent.

Additionally, the draft language is confusing, leaving open the question of what "documentation" organizations must provide upon request. The wording is so broad that federal agencies could interpret it as allowing them to conduct a full audit of organizations' research security programs for no specific reason. This could subject organizations to multiple audits a year, requiring undefined amounts of organizations' personnel time. Since organizations would only have 30 days to respond, this section should specify that federal agencies may request only a description of the research security program (as required by the Implementation Guidance). We recommend that the Standards stipulate that Federal agencies may only request additional information beyond a description of the research security program when there has been a research security incident related to a specific program funded by that agency. We further recommend that organizations be given a reasonable amount of time to respond to requests for such additional information (we suggest at least 90 days). Additionally, we recommend that all government agencies be subject to a uniform set of parameters for auditing or reviewing organizations' research security programs.

Foreign Travel Security

The travel security protocols are too broad and should be revised to apply only to scenarios that address "identified risks to research security" and that produce a "benefit that justifies any accompanying cost or burden," as stated in the NSPM-33 Implementation Guidance.

As written, the Foreign Travel Security section would impose a substantial burden while in most cases producing little benefit. The draft Standards require authorization in advance of international travel, regardless of whether the travel is related to federally-funded R&D or whether the travel is

to a country of specific concern. Authorizing each instance of international travel for all employees whose salaries are funded in part by federal funds—regardless of whether the travel is related to federally-funded R&D—would be burdensome and infeasible, given the amount of time and personnel required to review every travel request. UC's limited resources would be ill-spent reviewing requests to travel to countries that are not of specific concern, for purposes that have no relation to federally-funded R&D, or involve research areas not related to science and engineering. For the Standards to generate a benefit in proportion to the burden of the foreign travel security requirements, UC suggests the following changes:

- All references to "international travel" should be replaced with "covered international travel" for consistency and clarity.
- OSTP should revise the definition of "covered international travel" to mean travel that is both related to a federally funded R&D program *and* that is to a country OSTP believes might engage in "interference or exploitation." (NSPM-33, sec.1.) OSTP could create a list of countries of concern and refer to that list in the definition of "covered international travel," or the definition in the Standards could reference countries indicated in OFAC's sanctions programs, or an embargoed or sanctioned country listed by the EAR or the ITAR.
- Because "covered international travel" should pertain only to travel related to a federally-funded R&D award, this definition as well as that of "covered individuals" should be redefined to remove reference to individuals "seeking" federal funding and to "proposed" projects.

Lastly, we strongly suggest deleting "or to travel including electronic devices utilized for federally funded R&D or bought with Federal funding." This language is extraneous and confusing. If the definition of "covered international travel" is revised as suggested above to specify travel related to a federally-funded R&D program, then security briefings would always include "advice regarding electronic device security" for "electronic devices utilized for federally funded R&D."

Research Security Training

The Standards should require research security training only of "covered individuals" rather than "personnel" broadly. As many UC personnel have no direct connection to federally-funded R&D, this expansive requirement would be an inefficient use of resources on training that would have no benefit to research security.

Cybersecurity

The Standards should make clear exactly which baseline cybersecurity controls covered research organizations must implement. The Standards clearly list 12 required protocols but add unnecessary complexity with the reference to the National Institute of Standards and Technology (NIST) website. As written, the NIST reference could mean that covered research organizations must implement both the 12 protocols and the NIST standards and practices (of which there are many, applying to a variety of scenarios). Alternatively, the reference could be only an optional resource. For the avoidance of confusion, we suggest removing the reference to the NIST website.

In addition, OMB should clarify that the one-year implementation timeline only applies to the 12 protocols listed; it should not apply to unspecified NIST standards. If OSTP later determines that additional protocols are needed, OSTP should allow covered research organizations at least two

years to adopt newly established baselines or standards. Cybersecurity protocols should be replaced by a uniform security baseline adopted by science agencies funding fundamental research.

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 and use of compensating controls that manage risk. Institutions working in good faith to fulfill the protocols, 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.

Export Control Training

UC suggests revising the last two sentences of this section. For the second to last sentence, UC agrees that any export training should discuss situations where the fundamental research exclusion ("FRE") may not apply.[1] Nonetheless, stating that the FRE has "explicit limitations" is unclear because the Standards neither subsequently state nor reference any "explicit limitations."

In addition, UC suggests that OSTP delete the provided example scenario. This example does not focus on the core concept of the FRE, i.e., the research is to be published and shared broadly without restriction.[2] The analysis for FRE applicability and export license requirements is case specific. Rather than attempting to explain the nuances of the FRE and the complex application of export control law in the Standards, UC suggests OSTP revise the last two sentences to read:

> "The training must explain the boundaries of the fundamental research exclusion, specifically that even in the course of fundamental research, transactions, items, or activities may require export licenses, control plans, or other compliance approaches."

Covered research organizations are already required by U.S. law to comply with export control regulations, including federal regulations defining the FRE (see 10 C.F.R. § 810.3 and 15 C.F.R. § 734.13).[3] Therefore, the Standards need not attempt to explain rules regarding the application of the FRE or when an export control license is required. Instead, UC suggests keeping the scope of the Standards to guidance on training content as it relates to research security.

Definitional Appendix

For clarity, UC strongly suggests removing all reference to "senior/key personnel" from the definition of "covered individual." Various federal agencies define the terms "senior personnel" and "key personnel" differently. (Cf., e.g., the NSF GPG, defining senior personnel as a PI/co-PI or as a faculty member "who will participate in the project," with the NIH General Application Guide, defining senior/key personnel as "all individuals who contribute in a substantive,

[1] See University of California, Export Control Policy, p.8 (June 21, 2018) (listing examples of transactions and activities that may require export control licenses or control plans), *available at* https://policy.ucop.edu/doc/2000676/ExportControl.
[2] 81 Fed. Reg. 35586, 35589 (June 3, 2016), *available at* https://www.federalregister.gov/d/2016-12734/p-40. The Bureau of Industry and Security explain that the phrase "basic and applied research" was removed from the definition of "fundamental research" for clarity, but the scope remains the same. *Id*.
[3] See University of California, Export Control Policy, p.2 (outlining UC's approach to complying with export control requirements in the conduct of academic research and teaching).

meaningful way to the scientific development or execution of the project.") In particular, we suggest deleting the entire second sentence of the definition because it is confusing and does not add anything substantive to the first sentence. We also strongly suggest removing the words "proposed to be" from the first sentence, as persons would not yet contribute to a research project that has merely been proposed.