COGR

Council On Governmental Relations

An Association of Research Institutions

February 15, 2022

Submitted via Email to Addresses below and to ResearchSecurity@ostp.eop.gov

Linda Lourie, Assistant Director for Research and Technology at
Linda.S.Lourie@ostp.eop.gov
White House Office of Science and Technology Policy (OSTP)
Co-Chair, National Science and Technology Council Joint Committee on the Research Environment's Subcommittee on Research Security ("Subcommittee on Research Security")

Christina Ciocca Eller, Assistant Director for Evidence & Policy, OSTP at
Christina.C.Eller@ostp.eop.gov
Co-Chair, Subcommittee on Research Security

RE: Comments Concerning the January 2022 Guidance for Implementing NSPM-33

Dear Ms. Lourie and Dr. Eller:

The Council on Governmental Relations (COGR) is an association of 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at its member institutions. COGR has been extensively involved in assisting its member institutions in their efforts to ensure compliance with federal agencies' initiatives to address inappropriate foreign influence on federally funded research.

COGR appreciates OSTP's leadership of the collaborative efforts that produced the "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development" ("Implementation Guidance"). COGR also appreciates OSTP's hosting of the January 21st Implementation Guidance community briefing, which COGR representatives attended. During that briefing, OSTP and federal funding agency representatives encouraged community members to provide input regarding the Implementation Guidance, and we welcome this opportunity to provide comments. In this letter, we first set forth some general comments concerning the Implementation Guidance as a whole, followed by specific comments on the major sections of the document.

General Comments Regarding the Implementation Guidance

America has benefitted tremendously from the research partnership between federal funding agencies and academic research institutes. As the Implementation Guidance points out, one of the United States' most "enviable superpowers" is its ability to attract talented scientists and engineers, many of whom start their careers at our leading research universities. COGR and its member institutions understand both the value of international scientific partnerships to the United States' scientific enterprise, and the potential research security risks that certain improper collaborations may pose. We appreciate the Implementation Guidance's aim of mitigating these security risks, and we offer these suggestions as a means to improve the accomplishment of that goal.

Striking an Appropriate Balance through Use of a Risk-Based Approach: The Implementation Guidance discusses the importance of protecting core values of scientific research – objectivity, fairness, and transparency – and notes governments of some countries (including China, Russia, North Korea, and Iran) as having violated these norms. COGR and its member institutions fully endorse these values and promote them. At the same time, we recognize that any efforts to protect research values must do so in a way that fosters and protects the ability of federally funded researchers to participate broadly in international collaborations on fundamental research. Indeed, international collaborations confer tremendous benefits on the U.S. scientific enterprise,[1] and the freedom to engage in such collaborations is an important complement to America's "superpower" for attracting international science and technology talent.

The Joint Committee on the Research Environment (JCORE) January 2021 report "Recommended Practices for Strengthening the Security and Integrity of America's S&T Research Enterprise" ("2021 JCORE Report") recognized the need for balance in this area and advocated the use of a "risk-based approach that recognizes the benefit of open, international collaboration as well as the risk" and applies "protective measures commensurate with identified risks, accounting for both likelihood of occurrence and impact, weighed against tangible benefits" and "accompanying costs or administrative burden resulting from mitigation measures."[2] Although the Implementation Guidance, advises federal agencies to "incorporate measures that are risk-based, in the sense that they provide meaningful contributions to addressing identified risks to research security and integrity," the Guidance does not fully elaborate on all of the benefits of international collaborations to the U.S. scientific enterprise and the need to tailor measures to ensure that such benefits continue to accrue.

COGR urges OSTP to follow through on the 2021 JCORE Report's risk-based approach, by ensuring that research security requirements applicable to fundamental research take into consideration the fact that such research is published, presented, and broadly disseminated, and as such does not present the same security risk as research that is classified or subject

[1] American Physical Society, "Impact of U.S. Research Security Policies – U.S. Security and the Benefits of Open Science and International Collaborations" (Dec. 2021).
[2] 2021 JCORE Report at p. 4.

to export controls or similar restrictions. By employing a risk-based approach, research security measures can be configured so as not to unnecessarily limit federally funded researchers' opportunities to engage, in a fully transparent manner, in international collaborations on important fundamental research topics. A risk-based approach also supports the leveraging of existing risk-mitigation structures (e.g., existing federal standards on information and cyber security) to achieve transparent, efficient, and cost-conscious implementation of new agency requirements. Alternatively, use of a broad-brush, one-size-fits-all approach may have a chilling effect that needlessly dissuades U.S. researchers from engaging in collaborations with researchers in some of most scientifically advanced countries in the world, thereby precluding not only the researcher, but also the U.S. as a whole, from the benefits of broader scientific engagement.

Consistency: We cannot emphasize enough the importance of consistency in agency standards, forms, and instructions. We applaud OSTP's efforts to promote cross-agency consistency, and we appreciate the hard work that individual agencies have dedicated toward harmonization. Nevertheless, key differences persist in how agencies (and in some cases, the Implementation Guidance) address the disclosure of certain items/activities. COGR has described these differences in its "Summary of NSTC Guidance for Implementing National Security Presidential Memorandum 33 Disclosure Requirements." We urge OSTP to resolve these inconsistencies, which create confusion, compliance challenges, and impose significant researcher burden and institutional costs. Additionally, OSTP should ensure that agencies are consistent and transparent with respect to the identification of specific countries, institutions, and people of concern, including the use of any tools or lists used to identify persons/entities of concern.[3]

We also encourage OSTP to consider whether cross-agency consistency could be further promoted through the use of a "common rule" approach, similar to the Federal Policy for the Protection of Human Subjects.[4] Rather than have each agency individually develop and implement NSPM-33 requirements regarding disclosure and security programs, OSTP could lead agencies in the development of single "common" proposed rule for research security that federal agencies could then codify. In addition to promoting consistency, this common rule approach would ensure that the regulated community has a formal and robust process for reviewing and commenting on the proposed rule.

Ensuring Transparency About How the Government will Use the Information that is Collected: The foreword to the Implementation Guidance acknowledges that the federal government must next address how it will use the information that researchers disclose. This transparency is critical to the health of the partnership between research institutions and funding agencies. Just as researchers must be fully transparent in their disclosures,

---

[3] *See, e.g.,* Defense Advanced Research Projects Agency (DARPA), "Risk-Based Measures to Assess Potential Undue Foreign Influence Conflicts of Interest or Conflicts of Commitment – Rating Factors for Assessing Senior/Key Personnel Disclosures," which contains lists of persons/entities against which researchers' affiliations will be evaluated.

[4] U.S. Dept. of Health & Human Services, "Federal Policy for the Protection of Human Subjects ('Common Rule')."

COGR urges OSTP to require similar transparency from agencies on this topic. Along these lines, though the Implementation Guidance clearly prohibits discrimination against *individuals* based on ethnicity or national origin, the Guidance also acknowledges risks associated with some foreign *governments.* Thus, as previously noted, researchers remain fearful that *any* academic collaboration with researchers in certain countries may negatively affect the prospect for federal funding, even if it is a straightforward academic collaboration that does not have any "red flags." OSTP should instruct agencies to be clear regarding the impact of foreign collaborations on funding decisions for proposals for non-export controlled fundamental research, including any impact attributable to specific countries, individuals, and/or institutions. For example, if a federal agency will negatively view any collaboration that a researcher has with any foreign country when making funding decisions regarding a fundamental research proposal, researchers should be fully apprised of this fact prior to submitting their funding application. If, alternatively, an agency will negatively view only collaborations involving certain countries, or specific researchers/institutions in those countries, then these details must be clearly disseminated.[5]

Costs: COGR is spending considerable time analyzing the continuing cost impact and administrative burden on our community as institutions implement the NSPM-33 compliance requirements. ***This impact is significant***. Currently, we are working with a cohort of ten COGR member institutions to collect data on one-time and ongoing research security compliance costs, as well as data to understand the impact on researchers and other academic personnel. Our preliminary findings include the fact that institutions have been required to hire new staff and/or place significant additional responsibilities on existing staff to address disclosure requirements. In addition, many institutions have already made significant investments in process development/modification, information technology systems, and training to ensure researcher disclosure accuracy, and they will continue to do so as federal agencies implement NSPM-33.

The implementation of multiple, evolving, distinct agency requirements necessitates the development of multiple institutional forms, processes, and training, all of which equates to additional institutional and researcher time and effort, and unreimbursed institutional costs. We also are gathering and analyzing data to quantify the impact on faculty, including any reduced productivity and/or increased administrative burden. To limit the burden and cost of compliance, we once again urge OSTP to use all means at its disposal to achieve cross-agency consistency.

Specific Comments on Major Sections of the Implementation Guidance

(1) Definitions Section

Definition of Foreign Government-Sponsored Talent Recruitment Program" (FGTP): The definition of FGTP in the Implementation Guidance is exceptionally broad: "[e]ffort organized, managed, or funded by a foreign government, or a foreign government

[5] *See, e.g.,* DARPA, "Risk-Based Measures to Assess Potential Undue Foreign Influence Conflicts of Interest or Conflicts of Commitment, Factors for Assessing Senior/Key Personnel Disclosures" (Dec. 2, 2021).

instrumentality or entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position)." This definition is followed by examples of problematic attributes of FGTPs, but those attributes are not a part of the definition. Indeed, the definition encompasses activities that pose none of the described research security threats, nor is it limited to particular countries of concern. Rather, the definition is so extensive that it would encompass any foreign government's posting of available scientific/technical jobs on a website at which citizens from various countries may apply depending on the position. By casting such a wide net, the definition of FGTP places a job application to a Canadian university on the same footing as an application to a Chinese Thousand Talents Program despite the vast difference in the risks presented by these scenarios. We encourage OSTP to refine the definition to focus on behaviors of concern by limiting it as follows:

- Replacing the term "Foreign government-sponsored talent recruitment program" with "Malign foreign government-sponsored talent recruitment program" (MFGTP).

- Defining MFGTP as an activity that involves all, or some, specified, problematic attributes of FGTPs (e.g., unauthorized transfer of intellectual property, recruitment of individual to participate in the MFGTP, etc.). An example of this approach can be found in the definition of "Malign Foreign Talent Program" set forth in Section 10651(f)(4) of the America COMPETES Act of 2022.[6]

- Limiting the definition of MFGTP to specific countries that pose a threat.[7] The Implementation Guidance's definition of FGTP currently makes no distinction as to the country that sponsors or manages the FGTP, and, as noted in the example above, it is not clear that such a broad application of the term enhances research security. If, however, agency funding decisions will, in fact, be influenced by the existence of collaborations or affiliations with *any* foreign country, then scientists should be clearly apprised of this fact, so that they can evaluate the potential impact of what is, in essence, a United States non-compete clause.

(2) Digital Persistent Identifiers Section

COGR and its member institutions appreciate the Implementation Guidance's recognition that digital persistent identifiers (DPIs) may present an opportunity to reduce researcher burden in satisfying disclosure obligations. COGR also agrees with the Implementation Guidance's recognition that individual researchers should be empowered to control access to the information provided to DPI services. Although the use of a single DPI system presents obvious efficiencies, COGR also appreciates that the federal government may be unable to endorse the use of one private system over another. Accordingly, should a single DPI system

[6] H.R. 4521
[7] *Id.* at Section 10651(f)(3)

be impossible to achieve, COGR urges OSTP to develop criteria for the development and implementation of DPI system standards that eliminate any need for investigators to maintain accounts with multiple services that require time-consuming, duplicate data entry, an action that also may increase the chance of inadvertent inconsistencies. COGR also encourages OSTP to work with stakeholders who are interested in developing/piloting model DPI systems.

(3) Consequences for Violations of Disclosure Requirements

(a) Full Acknowledgement of the Limitations of Section 223 of the FY 2021 National Defense Authorization Act ("Section 223")

Section 223(c)(3) of the FY 2021 National Defense Authorization Act contains a "Special Rule for Enforcement Against Entities" (the "Special Enforcement Rule") that states that "an enforcement action," may be "taken against an entity" only when:

> (i) the entity fails to make a covered individual on an application for a research and development award aware of the individual's disclosure and certification obligations;
>
> (ii) the entity knew that a covered individual failed to make required disclosures and did not take steps to remedy the situation before submission of the funding application; or
>
> (iii) the head of a federal research agency determines that the entity is owned, controlled, or substantially influenced by a covered individual and that individual knowingly failed to make required disclosures.

The "enforcement actions" that are subject to this Special Enforcement Rule are detailed in Section 223(c)(2) and include the following actions taken against an entity or individual:

- Application rejection
- Award suspension/termination
- Temporary/permanent discontinuation of funding
- Temporary/permanent suspension/debarment
- Referral to the appropriate inspector general
- Placement in the Federal Awardee Performance and Integrity Information System
- "Such other actions against the individual or entity as are authorized under applicable law or regulations."

Despite Section 223's clear limitation of the foregoing enforcement remedies against entities to the circumstances described above, the Implementation Guidance is ambiguous on this point. Paragraph 7 under "Consequences for Violation of Disclosure Requirements" clearly references Section's 223's limitations on enforcement actions against entities, and the Guidance also states "that research agencies may apply other non-enforcement administrative actions and remedies to research organization for noncompliance with

disclosure requirements" including those listed in Table 3 of the Guidance. Yet, Table 3 inexplicably includes at least two actions that are specifically subject to the limitations of the Special Enforcement Rule: whole/partial suspension or termination of the federal award and withholding further federal awards for the project or program. Further, given that the Special Enforcement Rule encompasses "such other actions against the . . . entity as are authorized under applicable law or regulations," a strong argument can be made that use against entities of any of the actions and remedies set forth in Table 3 is limited to the circumstances described in Section 223(c)(3). COGR suggests that the Implementation Guidance be revised to clearly acknowledge the full extent of the statutory limitations placed upon enforcement actions against entities as described in Section 223.

(b) Section 117

The Implementation Guidance's section on consequences for violations also includes a description of the circumstances under which failure to disclose foreign gifts or contracts may result in the Department of Education's termination, suspension, or limitation of an institution's participation in the Higher Education Act (HEA) Title IV programs. COGR has previously asserted, and continues to maintain, that non-compliance with Section 117 reporting does not constitute a violation of an institution's participation in the HEA programs and program participation agreements under 20 U.S.C. 1094(a)(17).[8] Additionally, we wish to note that ongoing limitations of the Department of Education's portal for entering required disclosures have unnecessarily increased the administrative burden associated with complying with Section 117 reporting requirements. We hope that OSTP will consider reviewing community concerns with the portal as a part of its efforts to ensure institutions and researchers can "easily and properly comply" with disclosure requirements.

(3) Research Security Program Section

(a) Research Security Program Standards Should be Consistent and Flexible

COGR believes that any research security program standards should be grounded in the following basic criteria: cross-agency consistency, flexibility, and recognition of standards that are already in place for certain types of research (e.g., classified research). As with disclosure requirements, requiring inter-agency harmonization of research security program requirements will increase compliance and significantly reduce administrative burden. As previously noted, we believe that such consistency can be readily accomplished using a "common rule" approach.

Research security program standards also must provide sufficient flexibility for implementation in a wide variety of institutional settings. Security programs, of necessity, are influenced by institution size, security level of research conducted, and research type/discipline (e.g., biomedical research using human subjects v. basic science

[8] *See*, December 14, 2020 multi-association letter to U.S. Department of Education regarding Nov. 13, 2020 Notification of Interpretation (Docket No. ED-2020-OGC-0165).

research using an animal model). Agency regulations and guidance should recognize this flexibility by explicitly permitting institutions to implement a program in a manner and scope proportional to institutional risks.[9] An existing example of this type of flexibility is found in the longstanding Bureau of Industry Security's Export Compliance Guidelines. Finally, as OSTP leads efforts to develop standards, it should avoid layering on additional requirements for research segments that already have adequate security standards in place (e.g., export-controlled research, classified research).

Training: The content of any training modules that the government commissions for development should focus on promoting shared understanding of, and commitment to, common research security goals, including the scientific norms to which all researchers should adhere to promote transparency and a level playing field. Training should clearly elucidate for researchers what items/norms need to be protected in the case of fundamental research, which often entails lines that are difficult to discern between the protection of "intellectual capital" and ensuring compliance with federal data sharing and dissemination obligations. Training materials should encompass not only negative aspects of certain international collaborative relationships (e.g., negative attributes of FGTP), but also describe the characteristics of positive international collaborations and the means to achieve them. We note that the Implementation Guidance references the inclusion of insider threat training (as applicable), and we encourage OSTP to consider not only foreign threats in this regard, but also domestic threats such as lab infiltration by persons who desire to destroy research that they oppose (e.g., animal research, research using fetal tissue, etc.).

While government-provided training for a shared understanding of and commitment to common research security goals is a good starting point, training specifically targeting different types of institutional stakeholders (e.g., researchers, administrators, IT professionals, business offices) will be more effective than a "one size fits all" approach. Institutions will need to develop and provide training on their specific internal disclosure and research security processes. Knowing that institutions will need to develop this process-specific training, OSTP should consider how its training modules will intersect with and complement institution-specific training, including any commercially available training that is widely used by a large number of institutions (e.g., CITI Program training on Responsible Conduct of Research). Further, OSTP should consider how research security training will complement, and not duplicate, other training currently required/recommended by federal agencies (e.g., human subjects training, responsible conduct of research training, information security training, export controls training). Consideration also should be given to the time required to complete the training, effective modes of delivery, and specific audiences (e.g., graduate students, post-docs, faculty members, research administrators). Finally, institutions should be afforded the flexibility to tailor training to their particular institutional circumstances and needs.

We expect that it may take some time for the government to have training modules produced. In the meantime, many institutions have already been educating researchers on the need for

[9] For these reasons, we also believe that any research security program standards should not be considered a part of the Single Audit, given the tremendous variability in institutional profiles.

complete and accurate disclosures and the potential security issues raised by certain talents programs. Accordingly, OSTP should clearly delineate any additional topics that institutions should cover in this interim period, including any new or emerging security threats.

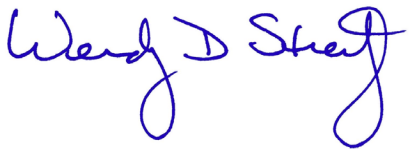
Cyber Security Standards: Flexibility is also vital with respect to cyber security standards. Many, if not most, institutions have cyber security programs in place that address requirements under existing federal standards, regulations, or frameworks. Many of these standards are accommodated by risk assessments that institutions regularly conduct for their facilities and systems and associated mitigation plans. Any mandated cyber security standards specific to research should permit institutions the ability to leverage their compliance with these other federal standards. The research security program also should allow them to determine applicability to institutional components based on risk assessment.

Conclusion

COGR will continue to work with its member institutions to analyze the Implementation Guidance and future guidance from OSTP regarding research security, as well as materials produced by individual agencies to implement NSPM-33. We value our partnership with federal agencies on this important topic and look forward to future opportunities to provide input.

If you have any questions concerning our comments, please contact Kris West, Director of Research Ethics & Compliance, at kwest@cogr.edu.

Sincerely,



Wendy D. Streitz
President

Copies to additional Co-Chairs of the Subcommittee on Research Security:
Dr. Steve Binkley, Department of Energy (DOE)
Dr. Rebecca Keiser, National Science Foundation (NSF), Co-Chair Subcommittee on Research Security
Dr. Michael Lauer, National Institutes of Health (NIH)