Submitted June 2023

MIT'S RESPONSE TO OSTP RESEARCH SECURITY PROGRAM STANDARDS

The Massachusetts Institute of Technology (MIT) provides the attached points for consideration in response to the government's Request for Information (RFI) on OSTP's proposed research security program standards ("Standards").

MIT takes security concerns seriously. For example, since 2019, proposed research collaborations with entities and individuals in China, Russia and Saudi Arabia have been subject to an elevated risk process review. That process and other MIT policies and views related to collaboration with China are described in a report MIT released in November 2022 (https://global.mit.edu/wp-content/uploads/2022/11/FINALUniversity-Engagement-with-China_An-MIT-Approach-Nov2022.pdf). Additional information about MIT's efforts to promote research security can be found on the website of the Vice President for Research (https://research.mit.edu/integrity-and-compliance/foreign-engagement).

In our comments, MIT is following the form indicated in the RFI. Responses will address one or more topics including (1) Equity, (2) Clarity, (3) Feasibility, (4) Burden and (5) Compliance. We note the corresponding number of the topic(s) to which each comment pertains.

A. **Uniform Certification Standard** [2,3,4]– MIT believes there should be a single set of research security Standards to which it will be required to certify, and appreciates OSTP's moves in that direction. But over the months since NSPM-33 was issued, several agencies (e.g., DOE, NASA, NIH) have adopted new agency-specific requirements[1] that should be eliminated or harmonized, to meet the goal of having a consistent, common set of standards. MIT recognizes that some specific research projects will necessarily require additional security protections, such as if sensitive or personally-identifiable information is involved. In such instances, any specific agency requirement(s) will be better implemented if treated as a contract term applicable to, and justified by the specific research agreement, rather than being cobbled onto the institution's overall certification requirements. The absence of a truly standard certification process introduces a substantial risk of requiring institutions to develop multiple certification processes, resulting in a lack of clarity and a substantial increase in burden due to inconsistencies and duplication of efforts.

[1] By way of example, DOE-funded programs require principal investigators to make individualized inquiry of all members of their research team in an effort to determine whether or not a member of the team acknowledges being connected to a malign foreign talent recruitment program. Requirements of this sort will tend to threaten the harmonization of requirements that NSPM-33 attempts to achieve.

B. **Standards Should be Risk-Based** [3,4] – Having a uniform certification standard should not mean that all research projects are treated identically, but rather that all projects that present a similar risk are treated similarly. The proposed Standards do not seem to take risk into account, resulting in an undue burden on researchers and on activities that pose little in the way of risk to research security. The lack of a risk-based approach could also damage security by misallocating resources and by provoking resentment among researchers. The Standards should recognize that risk level varies by the subject area of the research, the country/ies from which collaborators are participating and/or in which the research is being carried out, and details about the collaborator and the collaborator's institution.

C. **Consistency of Terminology** Used [2,4]: In the draft, there are a number of terms that appear to be used more broadly or more narrowly in different places. Consistency with respect to terminology will obviously improve clarity and reduce burden. We cite specific examples later in our comments.

D. **Clarity of Effective Date** [2,3,4]: OSTP should clarify whether the term "120 days from issuance of this Memorandum" means the date on which a final Memorandum is issued by OSTP; or the date(s) on which the final Memorandum is issued by individual funding agencies.

E. **Reporting of Violations**: MIT assumes that it is not the intention of the Memorandum to create any new process for reporting violations of research compliance requirements covered within the Standards. It would be very beneficial, for example, to clarify and deconflict how violation reporting envisioned within the Memorandum meshes with Voluntary Self-Disclosures of export control violations to BIS.

F. **Foreign Travel Security**

1. **Clarify Scope of "Covered Individual and/or Senior/Key Personnel" and "Covered International Travel"** [2,3,4]: The draft Memorandum requires institutions to establish international travel policies for covered individuals "engaged in federally funded R&D who are traveling internationally for organizational business, teaching, conference attendance, research purposes, or who receive offers of sponsored travel for research or professional purposes." As currently drafted, this requirement has many inconsistencies. For instance, the definition of "Covered International Travel" is "international, official business travel that contributes in a substantive, meaningful way to the development or execution of a research and development project proposed

to be carried out with a research and development award from a Federal research agency." The definition for "Covered Individual" that is used in the NSPM-33 Implementation Standards should be used consistently throughout the Standards.

2. **Covered International Travel** [3,4]: The definition should be limited to official business travel known to the institution that contributes in a substantive, meaningful way to the execution of the federally funded R&D project, and it should specifically state that international travel included in an award is considered disclosed and authorized. The draft definition applies to "faculty, staff, or students" seeking federal R&D funding, encompassing personnel who may be in the process of preparing funding applications and may not be known to the institution. The definition should be limited to Covered Individuals.
3. **Section Encompasses Travel that May Have no Nexus with Federal R&D** [2,3]: If the section does not employ and align these definitions as noted above, it will require institutions to maintain policies covering travel over which the institution may not have jurisdiction, e.g., sponsored travel for professional purposes that has no connection with federally funded research or with institutional responsibilities.
4. **Clarify What Must be Disclosed and Authorization Criteria** [2,3]: The section states that policies and procedures must include a "disclosure and authorization requirement;" however, no standards are provided as to what information must be disclosed. Further, as noted above, where international travel funding is included in a federally funded grant, it should be considered "authorized" without further action by the institution, and this should be clearly stated in the Standards.
5. **Standards are Not-Risked Based** [4]: The NSPM-33 Implementation Guidance issued last year (p.28) states that the disclosure, pre-registration and authorization requirements, security briefings, and assistance with electronic device security should be required "as appropriate." Yet the requirements in this section apply to all international travel, irrespective of the risk posed by the countries and/or specific locations traveled to, and the nature of the research being conducted. Imposing requirements on low- or no-risk situations would create an undue burden on institutions and could weaken security as noted in (B) above. The Standards should align travel security requirements with the risks actually presented by the travel and research.
6. **Scope of Electronic Devices Covered by Section is Not Feasible to Implement** [3,4]: The section states that "mandatory applicable security briefings" apply "to travel including electronic devices utilized for federally funded R&D or bought with Federal funding." It is not feasible for institutions to identify all electronic devices that might be used "for federally funded R&D," (e.g., personally owned laptops and cell phones). Greater alignment with 40 U.S.

Code § 11101(6) as to the scope of covered electronic devices would increase clarity and consistency with other government IT Standards.

G. **Research Security Training**

1. **Training Modules** [2,3,4]: The Standards should make clear whether training modules being developed under contract with NSF will be deemed sufficient to meet the training requirements and if not, the extent to which institutions will be expected to supplement them. Further, the section requires that training be "regularly" updated. It will be helpful to understand what would trigger the requirement to update.
2. **Training Frequency is Unclear** [2,3,4]: The section calls for research security training to be incorporated into existing programs such as Responsible and Ethical Conduct of Research training. While MIT welcomes this in concept, existing requirements vary with respect to initial training and refresher requirements. The timing of initial and refresher training should be clarified.
3. **Training Audience** [2,3,4]: The section needs to state who is required to receive training. Optimally, the requirements will be aligned with §10632(f) of the CHIPS and Science Act.
4. **Definition of Research Security Breach Finding is Unclear**: The section requires the conduct of "tailored training" in response to a "research security breach finding," but the term "research security breach finding" is not defined.

H. **Cybersecurity** [2.3.4]: The Cybersecurity Standards apply to "information systems used to store, transmit, and conduct federally funded R&D." The reality is that some systems such as student-owned laptops and other devices, and individually purchased cloud and cloud storage services, particularly useful in hybrid/remote work environments, are not within the ownership or control of institutions. The Standard should apply only to systems within the control of institutions.

I. **Export Control Training** [2,4]: The term "relevant personnel" is used in this section and nowhere else in the Standards. The term could be read to encompass "Covered individual or senior/key personnel," or a combination of that term along with other individuals across the "Covered Research Organization" that are involved in various systems and reviews of foreign sponsors, collaborators, and partnerships. That should be clarified.