National Science and Technology Council

Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government – Supported Research and Development

Report by Subcommittee on Research Security, Joint Committee on the Research Environment

Released: January 4, 2022

Overarching goal: Clarify and simplify how researchers disclose information to the federal government in a way that protects the nation's interests in both security and openness.

The guidance specifically focuses on five key areas addressed by NSPM-33:
1) disclosure requirements and standardization.
2) digital persistent identifiers.
3) consequences for violation of disclosure requirements.
4) information sharing.
5) research security programs.

Among some of the specifics contained in the guidance are that federal agencies shall:

- To the maximum extent practicable, standardize disclosure requirements, reporting forms and instructions for researchers across federal agencies that enable the development of tools such as electronic curricula vitae (CVs) and digital persistent identifier services (DPIs) and platforms to make compliance easy and uncomplicated. These forms and instructions are to be developed by federal agencies within 120 days (May 4, 2022).
- Incorporate Digital Persistent Identifiers (DPIs) into grant and cooperative agreement application and disclosure processes; and
- Adhere to specific guidelines for determining appropriate consequences for violations of disclosure requirements as deemed appropriate based upon the facts of the violation and consistent with applicable laws and regulations.
- Implement NSPM-33 guidance "…in a nondiscriminatory manner that does not stigmatize or treat unfairly member of the research community, including members of ethnic or racial minority groups."

Additionally, the report seeks to clarify specific circumstances when federal agencies may share information about violations and potential violations with each other consistent with due process, privacy consideration, and other applicable law. It also provides guidance concerning how research organizations awarded more than $50 million in a given year are to meet the research security program requirements called for in NSPM-33.

The report does not address key questions about how the government will use the information disclosed in making decisions about research funding and support.

Potential Impact on UC Research and Research Operations

1. Disclosure requirements could change which may impact the information collected in the Outside Activity Report (online disclosure system) and information provided to research agencies.

2. The guidance discusses and defines "outside activities", conflict of commitment and conflict of interest which may include non-research conflicts (e.g., foreign affiliations, participation in foreign government talent recruitment programs, participation in foreign programs whether or not sponsored by a foreign government, etc.). UC does not have any guidance on professional outside activities aside from collateral employment including no articles in the CBA discussing conflict of commitment and conflict of interest. A university-wide policy on outside professional activities may be warranted as this information will be required to be disclosed to both research agencies and UC.

3. The OoR will need to develop a certification process to notify each covered individual (UC researcher) who is listed on the research application of all disclosure requirements appropriately (leverage Kuali). Research Security and Ethics will work with Sponsored Research Services to ensure that each UC researcher listed on a research application is aware of the disclosure requirements, and that they revise and certify to their accuracy.

4. The guidance suggests that the use of digital persistent identifiers (DPI) will be the preferred vehicle to collect and share disclosure information uniformly across research agencies. This is a welcomed prospect as it will reduce administrative and researcher burden by harmonizing disclosure collection and review processes across agencies while protecting research integrity and security. UC already employs ORCID, a DPI entity. Universal access of ORCID at UC is available and encouraged, ensuring its universal adoption (or the identification and implementation of an acceptable alternative) will be paramount for compliance. It should be noted that ORCID is user friendly (and designed) for STEM-research; arts/humanities/social science researchers may struggle with utilizing this platform and may have to use a different platform.

5. An established and certified research security program will be required for any research organization that receives federal science and engineering support in excess of $50 million dollars per year. The Research Security and Ethics Office in OoR will need to formally document a program, standup a website and develop a training program that includes the following required elements: *cybersecurity, foreign travel security, insider threat awareness and identification, and export control training.*

6. **Mandatory and ongoing training** for all UC employees, students, and volunteers who contribute to "research, scholarly and/or creative work". It will be necessary to create awareness and to continue to foster a culture of transparency. The following items will need to be covered:

   a. Information required to be disclosed to research agencies and format (DPI).
   b. Process to correct omissions and inaccuracies in reporting.
   c. Penalties for failure to disclose.
   d. Information sharing of violators to research agencies.
   e. Cybersecurity awareness.
   f. Export control as appropriate.