OSTP Issues August Update on Research Security

NSPM-33 IMPLEMENTATION STATUS

On Aug. 31, 2022, the White House Office of Science and Technology Policy (OSTP) published an update on its blog regarding the implementation of National Security Presidential Memorandum 33 (NSPM-33), which it announced in January. OSTP's update highlighted four key topics:

- **Draft standardized disclosure requirements:** National Science and Technology Council's (NSTC's) Subcommittee on Research Security (SRS) released draft standardized data fields and instructions for pre- and post-award disclosures relating to biographical sketch and current and pending (other support) documents among researchers applying for federal funding, which will be piloted by the National Science Foundation (NSF).

- **NSTC outreach:** SRS engaged with the U.S. research community, hosting engagement hours in the spring of 2022, which were attended by a diverse mix of nearly 40 organizations. OSTP noted that further outreach by NSTC will continue.

- **DPI planning:** NSTC worked to develop policies related to NSPM-33's requirement for researchers to be registered with a digital persistent identifier (DPI), which included recent working groups led by OSTP and the Department of Energy (DOE) having discussions and designing a thoughtful, comprehensive approach to federal wide implementation.

- **Research security programs:** SRS has continued to clarify and specify the research security program requirement contained in NSPM (for research organizations that receive less than $50 million in federal science and engineering funding for more than two consecutive years). In addition, the CHIPS and Science Act of 2022 set forth additional guidance regarding the security training portion of research security programs.

Summary of Updates

Draft Standardized Disclosure Requirements and Revisions

NSF requests public comment within 60 days (due by 10/31/22)

- Items subject to comment include:

  – A common biographical sketch form, including data elements and associated instructions.

  – A common current and pending (other) support form, including data elements and associated instructions.

  – An Excel spreadsheet that summarizes all the data elements, as well as their data attributes.

- Comments are requested about:

  – The necessity of information
    proposed to be collected.

  – The accuracy of the estimate of the
    burden of new requirements.

    - NSF estimates that for an estimated
      47,900 proposals, if each contains
      four personnel who submit one
      biosketch and one current and
      pending each, that each will spend
      two hours, equaling approximately
      383,200 total annual burden hours.

- Suggestions for:

  – How to improve or automate
    information collection.

  – How to minimize the burden of
    providing information.

**Key Standard Disclosure Requirements
and Data Elements**

- Biographical sketch:

  – Removed "organizational affiliations"
    from activities to be disclosed.

- Current and pending (other) support
  requirements included:

  – Consulting outside of an
    individual's appointment.

  – Current or pending participation or
    applications to programs sponsored by foreign
    governments (as applicable per contract).

  – (new) Startup company based
    on non-proposing organization
    intellectual property (IP).

  – (new) Startup packages from a
    non-proposing organization.

- In-kind contributions not intended
  for use in the proposed project with
  an associated time commitment.

- Visiting scholars, postdocs, and/or
  students funded by another entity who
  will be involved in another project.

- A subset of in-kind support must be
  disclosed in facilities, equipment,
  and other resources, including:

  – Current or pending participation or
    applications to programs sponsored by foreign
    governments (as applicable per contract).

  – In-kind contributions in support
    of the proposed project.

  – Visiting scholars, postdocs, and/or students
    funded by another entity who will be
    involved in the proposed project.

- Copies of contracts or other supporting
  documentation relevant to the disclosed
  activities may be required.

**Refreshed instructions for pre- and
post-award inclusion of disclosures**

- Details on where each disclosure type should be
  entered in federal grant applications and reports

- An Excel document with the complete list of
  data elements and attributes was provided.

NSTC Outreach

**Almost 40 diverse research organizations
shared information with SRS, including:**

- Public and private colleges and universities.

- Nonprofit and professional organizations.

- Scholarly and advocacy organizations
  representing the Asian American, Pacific
  Islander, and Native Hawaiian communities.

The SRS anticipates releasing a public report this fall capturing the recommendations made and lessons learned. It anticipates adding engagement hours to hear from colleges and universities who identify as:

· Rural

· Historically Black

· Historically Spanish speaker-serving

· Tribal colleges and universities

· Other minority-serving institutions

· Regional colleges and universities

· Community colleges

Colleges and universities can email researchsecurity@ostp.eop.gov to express interest in participation in additional outreach sessions.

DPI Planning

Digital persistent identifiers (PID or DPI) will be required, including:

· ORCID (Open Researcher and Contributor ID) for all senior/key personnel in the application biosketch and in current and pending (other) support.

· Product persistent identifiers (e.g., digital object identifier URL for publication) for all products listed in the biosketch.

Research Security Programs

· The CHIPS and Science Act extends requirements regarding the research security training of NSPM-33 to all covered individuals applying to receive federal science and engineering funding as employees of institutions of higher education or other research organizations.

· OSTP expects to have specific training developed for research organizations, including:

– Detailed requirements regarding general research security training
– Foreign travel security
– Cybersecurity
– Export security

· OSTP anticipates publishing this guidance through the notice of the proposed rule-making process this fall.

· NSF, the Department of Defense (DOD), the Department of Education, and the National Institutes of Health (NIH) are collaborating for the creation of digital training content to meet the research security training requirements. The training will be freely and openly available for use by research institutions.

Actions You Can Take Now

As public comment on the draft disclosure forms is underway, and new details related to the implementation of NSPM-33 continue to emerge, institutions can mobilize to consider:

1. People and resource needs: Assess the impact of these new requirements for research administration and compliance teams. Determine what additional resources may be required in order to manage compliance, or if existing resources need to be redeployed.

2. Policies, procedures, technology, and data impacts: Review how these new requirements might challenge current processes and workflows.

   A. Disclosure requirements related to in-kind support, externally funded investigators (visiting scholars, postdoctoral fellows, and graduate students), and noninstitutional funding received by investigators may require access to data that is often not readily available to grant administrators. Compliance will involve a broader approach and stakeholders (e.g., contracting offices, human resources, graduate student affairs).

HURON CONSULTING GROUP®

B. Consider ways in which information can be shared across functional areas to meet new and emerging research compliance requirements.

3. Organizational models: Delegate the responsibility to implement, oversee, and monitor these regulations to live long term institutionally. Establish how your institution can best activate organizational readiness to comply with requirements that are pending finalization (e.g., disclosure requirements) or still in flight (e.g., research security programs and DPI use).

4. Communication: Activate training and education resources at your institution in order to facilitate regular communication about new disclosure requirements with faculty and research personnel.

5. Mission, strategy, and values: Engage thoughtfully with your leaders and the broader research community at your institution to determine how to balance academic freedom, diversity and inclusion, and compliance with federal guidance.

How Huron Can Help

Huron's team of research compliance experts has supported institutions with proactive assessments of foreign interference and research security and compliance programs, responding to both federal sponsor and enforcement agency investigations and delivering training for faculty, departments, and central office staff. Our team has deep expertise supporting research institutions by working to update and implement policies and procedures in response to regulatory updates.

Additionally, Huron Research Suite provides a long-term software solution to streamline collecting and managing various disclosures required by NSPM-33.

If you have concerns or questions regarding your institution's practices or readiness to implement these updates, contact one of our leaders today.

HURON

huronconsultinggroup.com