Updates on Research Security Policies and Practices in the U.S. Government

Office of Science and Technology Policy
Executive Office of the President

www.whitehouse.gov/OSTP
@WHOSTP

WHERE WE STARTED: NATIONAL SECURITY PRESIDENTIAL MEMORANDUM (NSPM)-33

- **Primary purpose of NSPM-33:**
  - Strengthen protections of U.S. government-supported research while maintaining an open environment in which to foster research discoveries and innovation

- **Practical application of NSPM-33:**
  - Develop a series of actions for Federal research funding agencies
  - Emphasize standardized policies for disclosures
  - Support transparency, researcher responsibility, and training for Federal researchers and those funded by Federal taxpayer dollars, especially through research security programs

NSPM-33 IMPLEMENTATION GUIDANCE GOALS

- **Reaffirm core values:** *openness, transparency, honesty, equity, fair competition, objectivity, and democratic values*
- **Acknowledge the seriousness of the challenge:** *some foreign governments are attempting to acquire our most advanced knowledge and technologies*
- **Communicate and apply policies in a clear and uniform way:** *policies must not fuel xenophobia or other forms of discrimination*
- **Continue welcoming international students, scholars, and collaborations:** *this openness is among the country's greatest strengths*

NSPM-33 IMPLEMENTATION GUIDANCE CORE PRINCIPLES

1) Protect America's **security** AND **openness**

2) **Be clear** so that researchers can easily and properly comply

3) Ensure that policies **do not** fuel xenophobia or prejudice

ENGAGEMENT WITH THE RESEARCH COMMUNITY

- We are grateful for the many opportunities we have had to engage and for all of your insights!
  - Hosted “Engagement Hours” over the course of last spring and heard from more than 35 organizations
  - Email us at **researchsecurity@ostp.eop.gov**!

NSPM-33 KEY PROVISIONS

1. **Disclosure Requirements and Standardization**
2. **Digital Persistent Identifiers**
3. **Consequences for Violating Disclosure Requirements**
4. **Agency Information Sharing**
5. **Research Security Programs**

DISCLOSURE REQUIREMENTS AND STANDARDIZATION

- With respect to research security, ensure federally funded **researchers** and **research organizations** provide the **appropriate information** regarding:
  - Potential conflicts of interest
  - Potential conflicts of commitment
- Advance **standardization** in disclosure requirements across agencies

LET US KNOW WHAT YOU THINK!

Federal Register Notice:

https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for

NSF Website (which houses this link!)

https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp

DIGITAL PERSISTENT IDENTIFIERS

- Encourage the use of **digital persistent identifiers** (DPIs), e.g., electronic CVs, in disclosure processes to bolster security while **reducing burden**

- We encourage creators of DPI services to include categories of information that **can identify and avoid financial conflicts of interest** and **conflicts of commitment**

CONSEQUENCES FOR VIOLATING DISCLOSURE REQUIREMENTS

- Consequences can include criminal, civil, and/or administrative actions

- A variety of factors should be considered when considering consequences:
  - Harm or potential harm to the Federal Government, U.S. taxpayers, and other National interests;
  - Intent;
  - Knowledge of requirements;
  - Pattern of violation vs. isolated incident;
  - Existence and timing of self-disclosure;
  - Policies, practices, and training available

- The Guidance encourages and ensures **mechanisms** for researchers **to correct** existing disclosures

INFORMATION SHARING WITHIN THE FEDERAL GOVERNMENT

- The Guidance directs **research agencies** to **share information** about violations of disclosure requirements
  - Must be consistent with due process, privacy considerations, and all other applicable laws

- Information sharing will take place through a **centralized** government portal, **SAM.gov**

RESEARCH SECURITY PROGRAMS

- NSPM-33 requires a **certification** from **research organizations** awarded $50M or more in federal awards that research security programs have been implemented

- Research security programs should include:
  - Cybersecurity
  - Foreign travel security
  - Research security training
  - Export control training, as appropriate

- The federal government will provide **standardized technical assistance** to develop the content of the programs

NEXT STEPS ON NSPM-33

- **Resolve feedback** on the standardized formats
- **Finalize** draft standards for the research security programs and **seek public feedback** on the draft
- **Coordinate** on communicating to researchers and research organizations **how agencies use disclosure information** in making decisions about research awards
- **Assess** agency implementation of NSPM-33 and **iterative improvement** of research security policies
- **Ensure alignment** with provisions coming from the CHIPS and Science Act

THE CHIPS AND SCIENCE ACT

- Signed into law on August 9, 2022

- A variety of research security provisions, incl.:
  - Foreign Talent Program participation and Malign Foreign Talent prohibition
  - Research security training requirements
  - A research security and training “analysis organization” (NSF to lead!)

CONNECTING WITH US

OSTP inbox for stakeholder inquires: ResearchSecurity@ostp.eop.gov