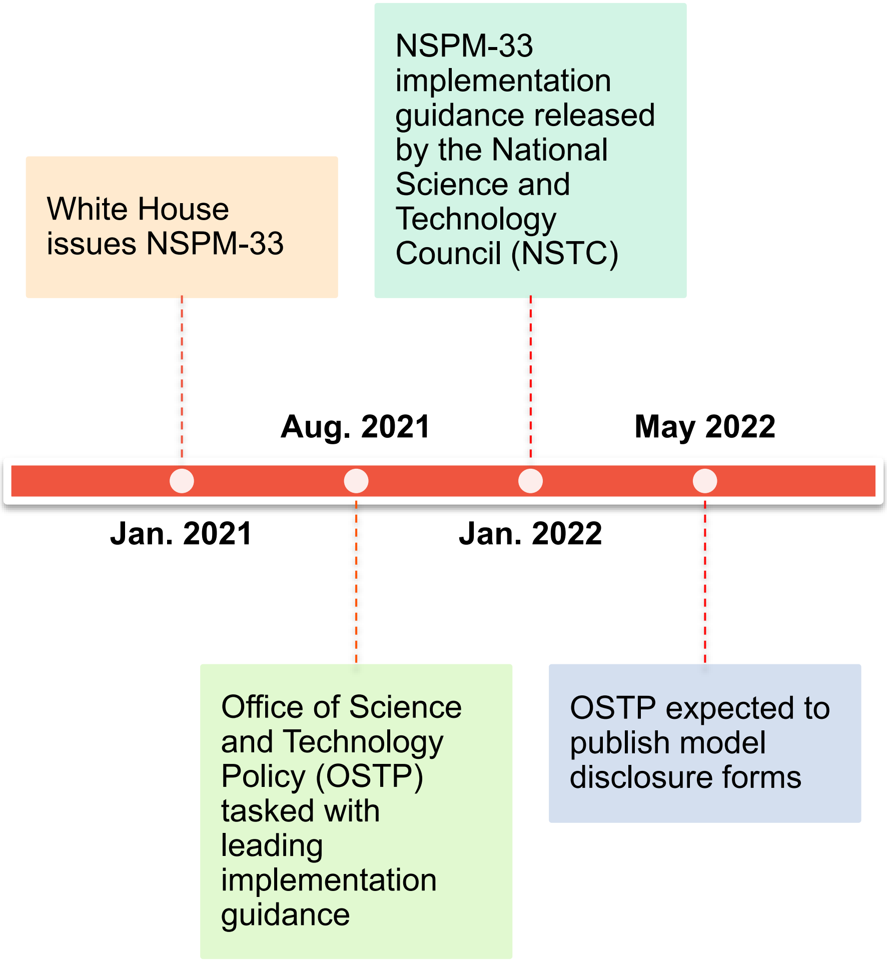
Northwestern
RESEARCH

NSPM-33 Implementation Guidance

Kate Cosgrove-Booth
Shandra White

What is NSPM-33?

- Presidential directive requiring federal research funding agencies to strengthen and standardize disclosure requirements for federally funded awards.
- The National Security Presidential Memorandum 33 (NSPM-33) also requires major institutions (≥$50M/year) receiving federal funds to establish research security programs.



Jan. 2021

White House issues NSPM-33

Aug. 2021

Office of Science and Technology Policy (OSTP) tasked with leading implementation guidance

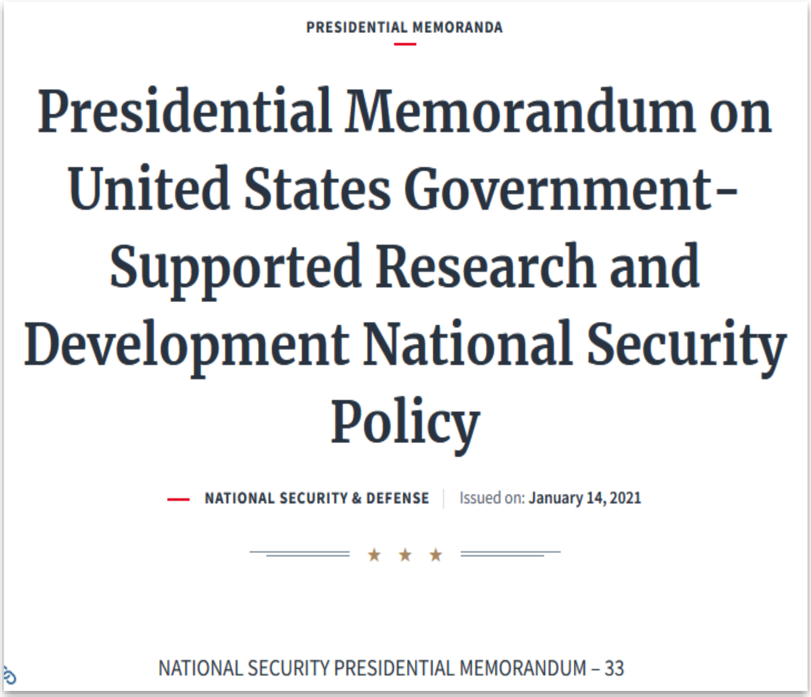
Jan. 2022

NSPM-33 implementation guidance released by the National Science and Technology Council (NSTC)

May 2022

OSTP expected to publish model disclosure forms

Jan. 2021: NSPM-33



PRESIDENTIAL MEMORANDA

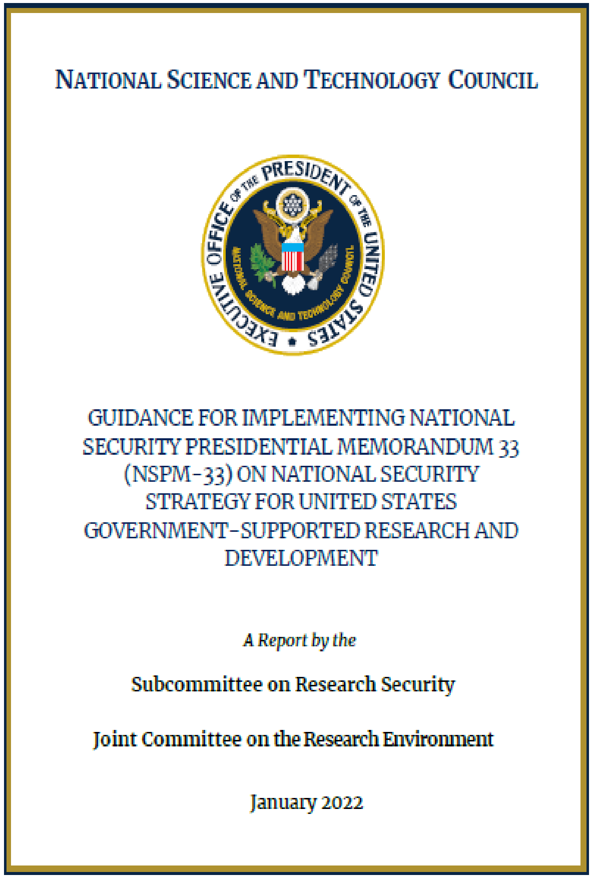
Presidential Memorandum on United States Government-Supported Research and Development National Security Policy

NATIONAL SECURITY & DEFENSE | Issued on: January 14, 2021

★ ★ ★

NATIONAL SECURITY PRESIDENTIAL MEMORANDUM – 33

Jan. 2022: Guidance for Implementing NSPM-33



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

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

General Implementation Guidance for Agencies

Provide clear, coordinated guidance that incorporates stakeholder input and does not excessively burden or unnecessarily harm researchers or research organizations.

Must implement NSPM-33 provisions and related requirements in a nondiscriminatory manner that does not stigmatize or treat unfairly members of the research community, including members of ethnic or racial minority groups.

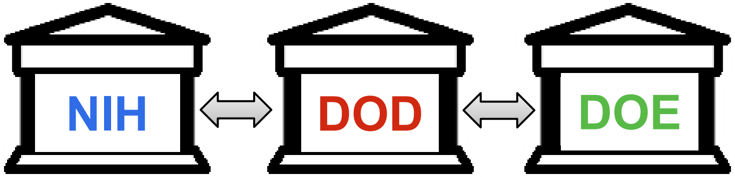
What's included in the NSTC Guidance?

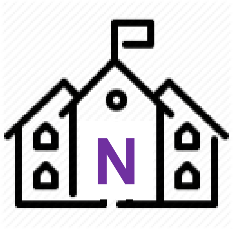
In addition to the general guidance, there is detailed guidance in five key areas addressed in NSPM-33.

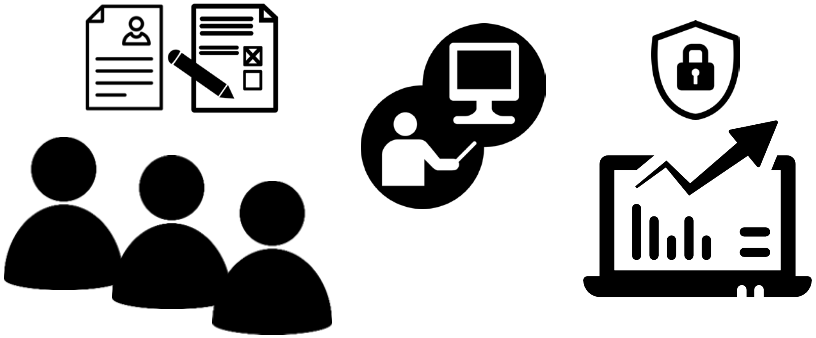
- ✓ Disclosure Requirements and Standardization
- Digital Persistent Identifiers
- 🚫 Consequences for Violation of Disclosure Requirements
- Information Sharing Across Agencies
- 🏛 Research Security Programs at Federally Funded Institutions

NSTC Guidance & Northwestern

- ✓ Disclosure Requirements and Standardization
- Digital Persistent Identifiers
- Consequences for Violation of Disclosure Requirements
- Information Sharing Across Agencies
- Research Security Programs at Federally Funded Institutions







DISCLOSURE REQUIREMENTS AND STANDARDIZATION

Background: Disclosure

NSPM-33 directives for agencies:	Require the disclosure of information related to potential conflicts of interest and commitment from participants in the Federally funded R&D enterprise
	Standardize forms for initial disclosures and annual updates as well as provide clear instructions to accompany these forms and minimize any associated administrative burden
Goal of guidance:	Provide clarity regarding disclosure requirements, disclosure process (e.g., updates, certification, and provision of supporting documentation), and expected degree of cross-agency uniformity

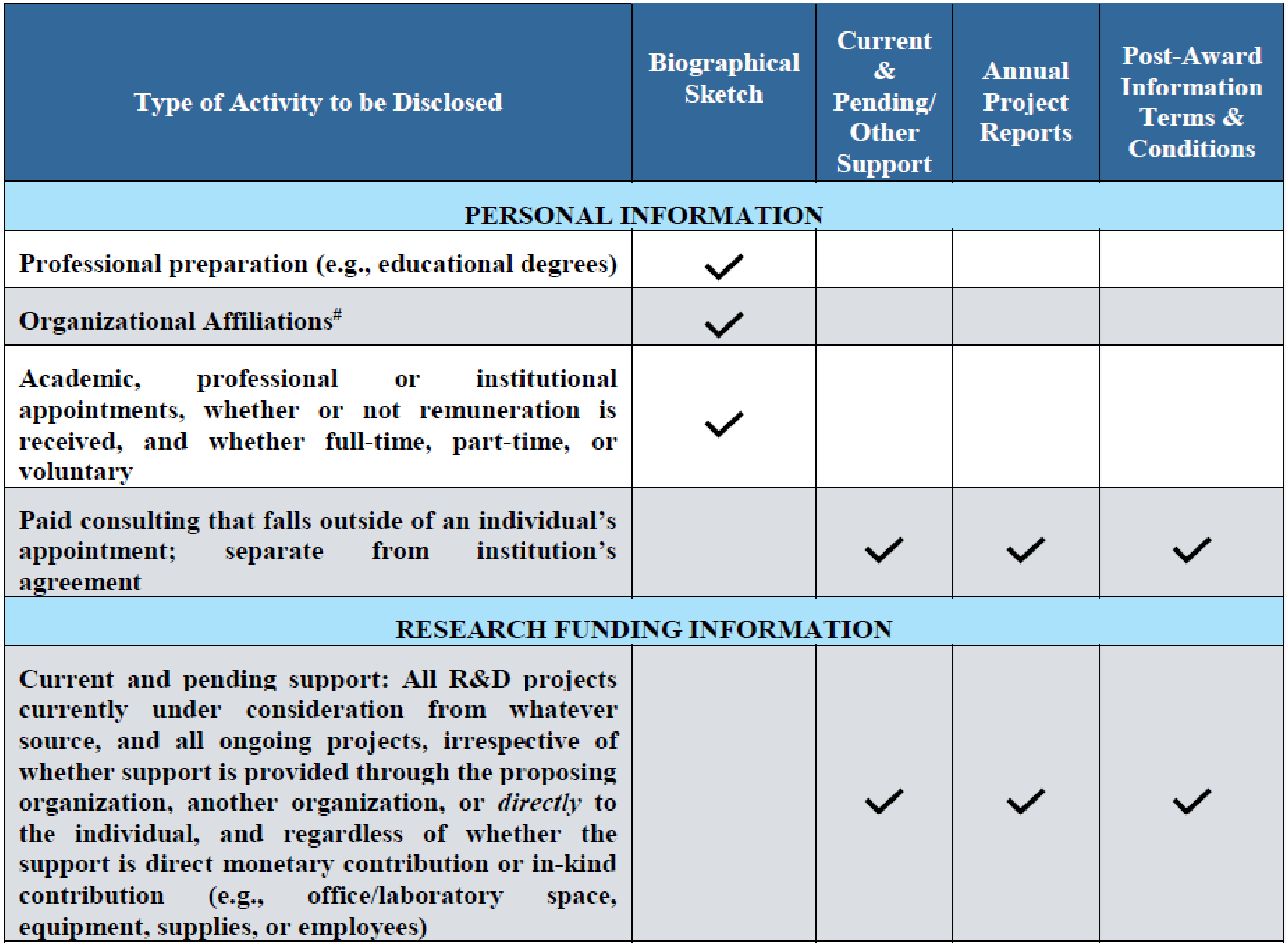
Standardization Across Agencies

Disclosure requirements and forms / formats

Collection of personal and professional information during application process

Standardized exclusions (e.g., gifts, mentoring)

Excerpt from Guidance:



Type of Activity to be Disclosed	Biographical Sketch	Current & Pending/ Other Support	Annual Project Reports	Post-Award Information Terms & Conditions
PERSONAL INFORMATION				
Professional preparation (e.g., educational degrees)	✓			
Organizational Affiliations[#]	✓			
Academic, professional or institutional appointments, whether or not remuneration is received, and whether full-time, part-time, or voluntary	✓			
Paid consulting that falls outside of an individual's appointment; separate from institution's agreement		✓	✓	✓
RESEARCH FUNDING INFORMATION				
Current and pending support: All R&D projects currently under consideration from whatever source, and all ongoing projects, irrespective of whether support is provided through the proposing organization, another organization, or *directly* to the individual, and regardless of whether the support is direct monetary contribution or in-kind contribution (e.g., office/laboratory space, equipment, supplies, or employees)		✓	✓	✓

Additional Guidance

For agencies:

- Additional guidance provided for disclosure requirements
- Requiring a "just-in-time" submission is at the discretion of the agencies

For research institutions:

- Certify that each covered individual who is listed on the application has been made aware of all relevant disclosure requirements
- Provide instruction to covered individuals on how to disclose information related to potential financial conflicts of interest

Implementation/Execution Example

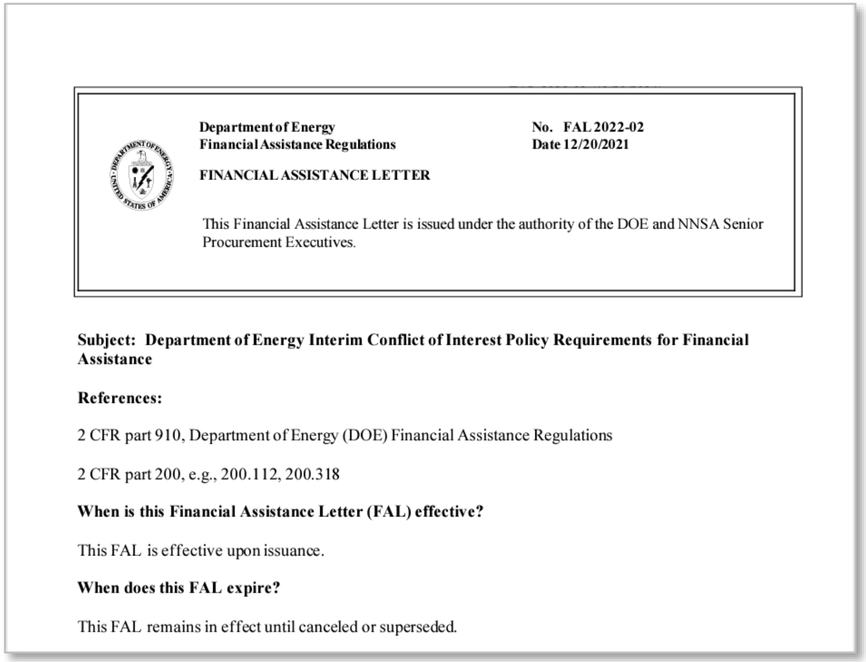
National Science Foundation

- Specific and direct inclusion of NSPM33 language and requirements in draft January 2023 PAPPG
- New sections:
  - Disclosure Requirements
    - Section II.B
    - Section II.D

- Required use of SciENcv for biosketches and current & pending support in tandem with encouraged use of an ORCID ID
- Required NDAA 223 Certification in SciENcv
- Specific reporting for direct or indirect participation in foreign government programs
- Implementation of Just-In-Time process

Implementation/Execution Example

Dept. of Energy



Department of Energy
Financial Assistance Regulations

No. FAL 2022-02
Date 12/20/2021

FINANCIAL ASSISTANCE LETTER

This Financial Assistance Letter is issued under the authority of the DOE and NNSA Senior Procurement Executives.

Subject: Department of Energy Interim Conflict of Interest Policy Requirements for Financial Assistance

References:

2 CFR part 910, Department of Energy (DOE) Financial Assistance Regulations

2 CFR part 200, e.g., 200.112, 200.318

When is this Financial Assistance Letter (FAL) effective?

This FAL is effective upon issuance.

When does this FAL expire?

This FAL remains in effect until canceled or superseded.

Specific and direct inclusion of NSPM33 language and requirements in Interim COI Policy Requirements.

"…DOE established the attached interim COI policy governing financial conflicts of interest and organizational conflicts of interest concerning applicants for, and recipients of, Federal financial assistance awards from DOE (Appendix 1).

To minimize the implementation burden on non-Federal entities, the interim COI policy is largely aligned with the long-standing conflict of interest regulations established by the Public Health Service at 42 CFR part 50, Subpart F."

Disclosure Requirements

Observations and Considerations

- ❖Guidance provides clarification on items to be included in or excluded from disclosures
- ❖Some inconsistencies exist between OSTP Guidance and individual agencies' *current* guidance, which will need to be either resolved or justified.
- ❖Disclosure is required to the institution (Northwestern) and federal agencies depending on the type of information

Application Considerations

- ➢How might the disclosure requirements impact **your** work?
- ➢What might be the implications for our campus?

DIGITAL PERSISTENT IDENTIFIER (DPI)

Background: DPIs

NSPM-33 directives for agencies:

Establish policies regarding requirements for individual researchers supported by or working on any Federal research grant to be registered with a service that provides a digital persistent identifier for that individual

Standardize forms for initial disclosures as well as annual updates, integrating digital persistent identifiers wherever appropriate and practicable

Goal of guidance:

Describe how research agencies will incorporate digital persistent identifiers (DPIs) into disclosure processes to bolster research security and integrity while reducing administrative burden

DPI Implementation:

Research agencies should…

Work to implement DPIs into their electronic systems and processes as quickly as is feasible

Provide the option to submit required disclosures via a DPI service for applications for grants and cooperative agreements as well as consider a DPI option for non-grant (e.g., contracts) mechanisms

But not require that individuals provide any public disclosure through the DPI

DPIs

Observations and Considerations

- ❖Guidance indicates that agencies should permit application processing without a DPI service.
- ❖Business processes impacts could be significant.
- ❖DPIs could be used at multiple points in award life cycle.

Application

- ➢How might the disclosure requirements impact **your** work?
- ➢What might be the implications for our campus?

CONSEQUENCES FOR VIOLATION OF DISCLOSURE REQUIREMENTS

Background: Consequences

NSPM-33 directives for agencies:

Agencies shall ensure appropriate and effective consequences for violation of disclosure requirements and engagement in other activities that threaten research security and integrity.

Depending on the nature of the violation, agencies may consider a range of consequences. (In addition to these measures, civil and criminal penalties under U.S. Federal and State laws may apply.)

Goal of guidance:

Provide guidelines for determining appropriate consequences, consistent with applicable laws and regulations, while preserving an appropriate level of flexibility for agencies and research organizations

Consequences

- Violation of disclosure requirements may lead to criminal, civil, and/or administrative consequences.

- Potential administrative actions may include (but not limited to):

Rejection of an R&D award application

Suspension or termination of an R&D award or preserving the award, but requiring that individual(s) do not perform work under the award

Placement of the individual or research organization in the System for Award Management (SAM) or Federal Awardee Performance and Integrity Information System (FAPIIS)

Administrative Actions Against Organizations

- Disclosure burden is on individuals
- An administrative action may be taken against an organization *only* in cases in which the organization:
  - Did not meet requirement to certify that covered individuals have been made aware of disclosure requirements
  - Knew that a covered individual failed to disclose required information and did not take steps to remedy such nondisclosure before the application was submitted
  - Is determined to be owned, controlled, or substantially influenced by a covered individual; and such individual knowingly failed to disclose required information.

Consequences

Observations and Considerations

❖ Burden placed on both the individual and the research organization

❖ Agencies need to provide information about administrative remedy and enforcement processes.

Application

➢ How might the disclosure requirements impact **your** work?

➢ What might be the implications for our campus?

INFORMATION SHARING

Background: Information Sharing

NSPM-33 directives for agencies:

Agency heads shall share information about violators or those whose activities demonstrate an intent to threaten research security and integrity with other Federal agencies/departments

When appropriate, agency heads should consider notifying other Federal funding agencies in cases where significant concerns have arisen but a final determination has not yet been made

Any sharing should be consistent with privacy laws and other legal restrictions

Goal of guidance:

Provide clarity regarding circumstances when and mechanisms by which agencies may share information regarding violations and potential violations

Circumstances for Sharing Violations

Research agencies **should share information** about violations or potential violations of disclosure requirements:

- When an agency identifies something potentially relevant to another research agency's management of funding
  - *E.g.*, Identical proposals from one or more PIs, where one or more is funded by other research agencies.
- Once administrative or enforcement action is taken
- When referring to an appropriate law enforcement or other agency or entity for further investigation and/or consideration of enforcement or administrative action
- In support of risk analysis and lessons learned

Information Sharing

Observations and Considerations

- ❖Concern about sharing of information prior to a final determination; irreparable or inappropriate harm
- ❖Roles and responsibilities need to be defined
- ❖Information needed about due process, privacy considerations, and more

Application

- ➢How might the disclosure requirements impact **your** work?
- ➢What might be the implications for our campus?

RESEARCH SECURITY PROGRAMS

Background: Research Security Programs

NSPM-33 directives for agencies:	Requirement that research institutions receiving Federal science and engineering support over $50 million annually certify that the institution has established and operates a research security program.
Goal of guidance:	Provide clarity regarding research security program requirements, expectations for recipient organizations, and how agencies will contribute to program content development

Research Security Program Required Elements

- Cybersecurity
- Foreign travel security — International travel policies & records
- Research security training, including insider threat training where applicable
- Export control training (as appropriate)
- Designated research security point of contact with a publicly accessible means to contact that individual (e.g., website)

Research Security Program Development & Implementation

Timeline:

- Organizations should establish a Research Security Program within one year from the date of issuance of the formal requirement to comply

Content:

- Federal government will provide technical assistance in the development of training and tools

Flexibility:

- Organizations should be provided flexibility to structure their Research Security Program to best meet their particular needs

Implementation/Execution Example

National Science Foundation

- Specific and direct inclusion of NSPM33 language and requirements in draft January 2023 PAPPG
- New sections:
  - – Research Security
    - Section IX.C

- Outlines objectives of NSF Research Security policy and initiative
- Coordination with US Government interagency partners
- Organizational requirement for AOR to submit failures to disclose current support or in-kind within 30 days
- Updating of C&P in annual and final project reports

Research Security Program

Observations and Considerations

- ❖NSPM-33 cybersecurity requirements and alignment with upcoming DOD requirements.
- ❖Terms to be defined, e.g., “covered international travel”
- ❖Training - research security & export control - will be required for relevant personnel.

Application

- ➢How might the disclosure requirements impact **your** work?
- ➢What might be the implications for our campus?

Research Security Program Requirements

Policy & Systems

- 14 requirements for safeguarding information systems
- International Travel Policy
- Pre-registration Requirement (?)
- Records for "covered international travel"
- Security briefings and electronic device programs

Training

- Research Security Training on threat awareness and identification
- Export Control Training for personnel that conduct work subject to export controls to include review of foreign sponsors and collaborators

Resources

- National Security Presidential Memorandum-33
- 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
- COGR summaries of NSPM-33 guidance
- NSF Draft Proposals & Award Policies & Procedures Guide

Wrap-up

Questions?

Contact Information

- Kate Cosgrove-Booth, k-cosgrove@northwestern.edu, (847)491-4163
- Shandra S. White, shandra.white@northwestern.edu, (312) 503-7955

Thank you for joining us!