FEDERAL DEMONSTRATION PARTNERSHIP
Redefining the Government & University Research Partnership

January 2022 Release of NSPM-33 Guidance (*Guidance for Implementing National Security Presidential Memorandum 33*)

Presenters:

Jim Luther, FDP

Lori Schultz, University of Arizona

Pamela Webb, University of Minnesota

January 13 , 2022 (3-4:15 EST)

Description

This session will include an overview of the NSPM and recent progress (per the initial 1/14/21 Pres. Trump NSPM communication and Dr. Lander's recent communications) and initial observations by the FDP Foreign Influence Working Group (FIWG) on the recently released Report entitled "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for the United States Government-Supported Research and Development".

We will be using a Thought Exchange to gather your input and concerns and the output of this session will be provided to federal partners to support future discussions.

We want to hear your thoughts!

As you listen throughout today's session, what concerns do you currently have related to NSPM 33 Implementation Guidance from OSTP?

https://tejoin.com/scroll/606671899

Click on the link and you will be walked through how the exchange works. We will put the link in chat so you can use anytime you have a thought during this session

We will keep this exchange open after the session and send a follow-up email after the meeting

August 10th Lander Blog Post

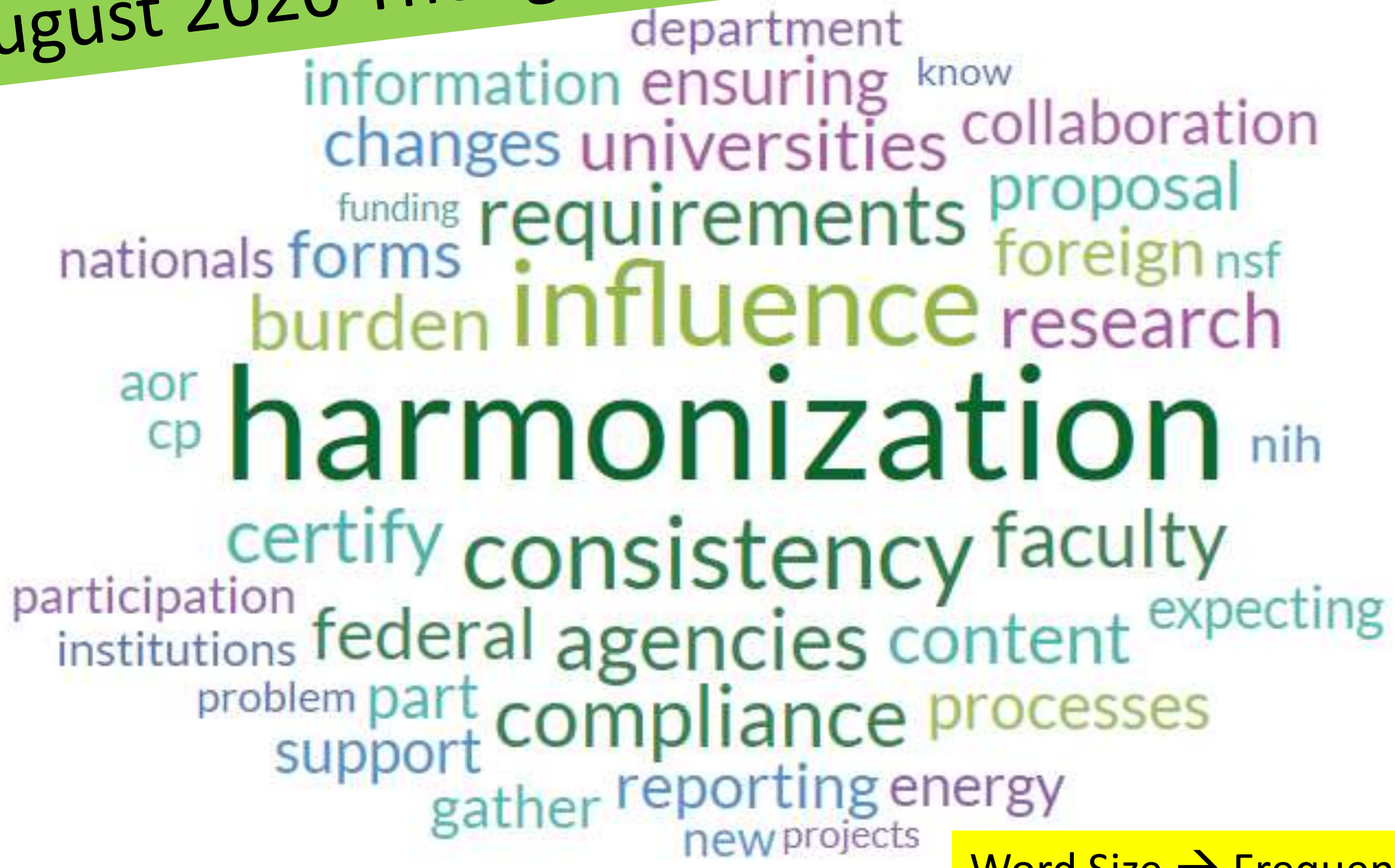
https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/

“The Office of Science and Technology Policy (OSTP) is working on how to implement NSPM-33 effectively, rigorously, and uniformly across the federal government in a way that protects the nation’s interests in both security and openness. Over the next 90 days, OSTP will develop clear and effective implementation guidance for NSPM-33 ..

1. Disclosure Policy
2. Oversight and Enforcement
3. Research Security Programs

Areas of FDP Interest

August 2020 ThoughtExchange



Word Size → Frequency
Word Color → Related Words

Let’s Dissect ..

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

Or navigate to: https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

Top 11 Take-Aways List

1. Strong potential for genuine harmonization and reduction of admin burden (strong role for)
2. Focus on clarity of expectations (first for agencies, then for us) -> training -> disclosure/ awareness -> enforcement
3. Obligation for complete, current and accurate information now shared between researchers and organizations
4. Unequivocable commitment to non-discrimination and fair treatment for all members of the research community
5. Technology (e.g., DPIs) paves the path for downstream elimination of "current and pending/other support" forms and biosketch forms

Top 11 Take-Aways List (cont’d)

6. Mandatory disclosure of foreign talent program applications or participation adds transparency
7. Enforcement of new requirements underscores importance and clarifies roles and responsibilities
8. Tension continues between privacy (particularly mid-inquiry) and transparency/information sharing
9. Funding for these important initiatives remains unsolved
10. Definitions for consulting and gifts continue to need further refinement and clarification
11. Disclosure requirements will extend to peer reviewers and advisory panels

Excerpt from Foreword by OSTP Director Eric Lander

- *"As a next step, I am now directing federal agencies to work together within the next 120 days to develop model grant application forms and instructions that can be used (and adapted where required) by any federal funding agency."*

- Government needs to clearly describe what it needs to know
- Researchers need to report the same information in the same way to the greatest extent possible, regardless of which funding agency they're applying to
- Software developers can then make tools to enable researchers to populate digital CVs

Purpose of Implementation Guidance Doc

- **Does not operate to bind** any department or agency of the US government or the public
- **Agencies expected to use NSTC to coordinate their implementations**
- Agencies expected to integrate their requirements with 2021 NDAA Sec 223 and Section 117 of HEA of 1965
- No budget guidance (use normal OMB budgetary, legislative and administrative processes)
  - Do not assume support in future budgets

Detailed Guidance Areas

1. Disclosure Requirements and Standardization
2. NEW Digital Persistent Identifiers
3. Consequences for Violation of Disclosure Requirements
4. NEW Information Sharing
5. Research Security Programs

Stakeholder Involvement

- ***"Agencies should engage with the research community throughout the implementation process and should consider stakeholder and community input and concerns."***

- ***"Engagement should include testing, piloting, and the solicitation of feedback during development of policies and forms, where practicable."***

General Guidance

- Regulations, policies and procedures should not be retroactive nor impose “excessive” administrative burden
- Measures should be risk-based (offer meaningful contributions to addressing risks relative to cost and burden)
- NSPM REQUIREMENT **Implementation MUST NOT stigmatize or treat unfairly members of the research community, including members of ethnic or racial minority groups**

1. Disclosure Requirements

OBJECTIVE - Provide clarity regarding:

- **Disclosure requirements**
  - who discloses what, relevant limitations and exclusions
- **Disclosure process**
  - updates, corrections, certification, and provision of supporting documentation
- **Expected degree of cross agency uniformity**

1. Standardization of Disclosure Requirements

- Disclosure requirements will be standardized across research agencies to the greatest extent possible

- Variations should be limited to:
  - (a) required by statute or regulation
  - (b) more stringent protections are necessary for protection of R&D that is classified, export-controlled, or otherwise legally protected
  - **(c) other compelling reasons consistent with individual agency authorities and as coordinated through the NSTC**

1. Disclosures Required

- PIs and Senior/Key Personnel must disclose:
  1. Organizational Affiliations/Employment
  2. Positions/Appointments
  3. NEW **Foreign Government sponsored talent recruitment programs**
  4. Current and Pending Support/Other Support

Program Officers, Intramural Researchers, Peer Reviewers, and Advisory Committee/Panel Members will also have to disclose all/most of this

1. Disclosure Forms and Formats

- Disclosure forms and formats will be standardized across research agencies to the greatest extent practicable
    - **Research agencies that adopt the standard requirements and processes should collect identical data elements**
    - Templates will be developed for biosketch and current and pending support/other support forms, leveraging existing forms as much as possible
    - Templates will include designation of "covered" individual per NDAA 223.
    - Broader classes of individuals (e.g. students) should generally not be included in disclosure requirements (except when deviations are necessary)

1. Potential Disclosure Refinements for some agencies

- Report paid consulting ONLY if it falls outside of an individual's appointment parameters (what is allowed or approved by the home institution)
- Current or pending participation in, **or applications to**, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs
- Visiting scholars, students, and postdocs funded by an entity other than the grantee institution
- Certification by an individual that the information disclosed is accurate, current, and complete
- Travel supported/paid by an entity other than the grantee institution to perform research activities with an associated time commitment

1. Potential Disclosure Changes or Refinements (continued)

- FCOI information should include private equity, venture, or other capital financing
- If required by law or policy, FCOI info may need to be disclosed both to the research agency and the home organization

1. Exclusions from Disclosure Requirements

- Completed support (including recently completed)
- **Consulting permitted by an individual's appointment and consistent with the proposing organization's "Outside Activities" policies and procedures**
- Honoraria (defined)
- Gifts (defined)
- Mentoring as part of appointment
- Teaching commitments at the recipient organization
- Academic or calendar year salary earned at the recipient organization

1. Specific Disclosures

- Footnote says, “Notwithstanding any exclusion from research agency disclosure requirements, research organizations typically require disclosure of paid consulting for consideration of potential FCOI. Agencies and research organizations should ensure that scientists do not inappropriately characterize research activities or involvement in foreign government-sponsored talent recruitment programs as consulting. **Authorships or co-authorship on a scientific or technical published paper or posted pre-print would be one manifestation of an activity that involves research**.”

1. Foreign Disclosures

- **Disclose applications or participation in programs sponsored by foreign governments, instrumentalities, or entities associated directly or indirectly with a foreign government (i.e., foreign governments or foreign government instrumentalities or entities)**

- Notes that participation in other types of foreign programs may still require reporting under other categories, such as affiliations, appointments or other support

1. Gift Definition

- **Compensation or consideration that are provided with terms and conditions and in support of R&D activities are not considered gift**s and must be disclosed by researchers as current and pending support
- Gifts are resources provided with no expectation of anything in return (e.g., time, services, specific research activities, money)
- Section 117 may still require disclosure through that process

1. Disclosure Timing and Updates

- Initial disclosure timing (at proposal or JIT) at discretion of agency
- Updates "should" occur:
  - Prior to award of support
  - Annually
  - More frequently or promptly where the agency deems appropriate to account for individuals' changing circumstances
  - NEW **The addition of covered individuals to funded research teams**
  - NEW **Potentially during post-award reporting or as a condition of receiving final increment of funds**

1. Disclosure Corrections

- Correction process required, communicated clearly, and must be simple and straightforward
- Required to be available at both the pre-award and post-award stages
- May include standard award terms and conditions

1. Disclosure Certifications

- **NSTC Subcommittee on Research Security will provide standardized certification language for potential adoption by agencies and organizations**
- False representations may be subject to prosecution and liability pursuant to (but not limited to) federal laws named in the document

2. DPI - Digital Persistent Identifiers

- Timing: **Within one year of the date of this memorandum**, funding agencies shall establish policies regarding requirements for individual researchers to be registered with a service that provides a digital persistent identifier for that individual.

- Terms interchangeably used are Digital Persistent Identifiers (DPIs) or Persistent Identifiers (PIDs)

2. DPI Concept

NEW

- Researcher maintains information required for disclosure on an individual “profile” or “record” maintained by a DPI service and including a DPI
- Researcher provides their DPI, authenticates their DPI through a DPI service, and authorizes the research agency to access their information (replaces form submission) for original + updates
- Researcher certifies DPI profile is complete, current and accurate
- Agency variants disclosed manually or via DPI profile

KIC

2. DPI Options

- Research agencies “should” provide the option of using a DPI service for disclosure but “may” retain the option for non-DPI submissions
- Research agencies may not make DPI services mandatory
- DPI services provided by private entities should be used to the greatest extent possible
- Research agencies are encouraged to ensure that one or more common DPI services is available across agencies
- The guidance provides common/core standards for DPI services
  - **Includes a requirement that the service be provided at no cost to the researcher**
  - Requires interoperability standards
- The DPI option should provide the lowest administrative burden for researchers, research organizations and research agencies

3. Consequences - Enforcement of Disclosure Requirements

- Range of consequences including criminal, civil and/or administrative actions
- Violations should be investigated by the agency Inspector General (IG) and referred as needed to the Department of Justice
- Agencies should document procedures, including roles and responsibilities for addressing disclosure failures
  - NSTC Subcommittee will create a standard operating procedure template
  - Self-disclosure taken into consideration
  - **Public disclosure** when warranted

3. Consequences - Disclosure Enforcement Actions

- Administrative Actions
  - Suspension and debarment of researchers or research organizations
  - Enforcement actions in 2 CFR 200
    - 200.206 Agency Review of applicant risk
    - 200.208 Imposition of specific conditions
    - 200.339 Remedies for non-compliance
    - 200.340 Termination and 200.341 Notification of Termination
  - Other enforcement actions
    - Rejection of a proposal
    - Suspension or termination of an award
    - Removal of a researcher from an award
    - Removal of a researcher from review panels or fed employment
    - Citation of the researcher or organization in SAM or FAPIIS
    - **Suspension or denial of Title IV funds**

3. Consequences - Factors Taken into Consideration

- Harm or potential harm to agency or national interests
- Intent of the offender
- Offender’s knowledge of the requirements
  - Policies, procedures, and training available to the offender
- Pattern or isolated incident
- Existence and timing of self-disclosure
- Other mitigating factors

3. Consequences - Notice and Due Process

- **Research agencies intending to take action must notify each individual or research organization**
  - Specific reasons for the action
  - Opportunity and process to contest the proposed action
- Safeguards for research organizations – adverse actions ONLY in case where:
  - The organization did not meet the requirement to certify that covered individuals have been made aware of disclosure requirements
  - The organization knew that a covered individual didn't disclose but didn't take steps to remedy the non-disclosure before the application was submitted
  - The agency head believed the organization is owned, controlled, or substantially influenced by a covered individual and that individual knowingly failed to disclose required information

4. Information Sharing

Purpose: Provide clarity regarding circumstances when agencies may share info regarding violations and potential violations, and provide assurance regarding privacy and other legal protections

Share when:

1. **Potentially relevant to other agency management of federal funding**
2. Once an administrative or enforcement action is taken
3. In support of risk analysis and lessons learned (to reduce risk of re-identifying individuals)

4. Information Sharing

- Agencies should share information **prior** to a final determination for reasons on preceding slide
  - After consultation with privacy officers, may develop new routine uses for agencies to share potential and actual violations
- Mechanisms permitted for sharing include:
  - SAM (debarment, suspension, voluntary exclusion)
  - FAPIIS (criminal, civil, admin proceedings, admin agreements, terminations for default, cause or material failure to comply)
  - Federal Register, agency websites
  - **Publicly share information of results of risk analyses and administrative remedy and enforcement processes**

5. Research Security Programs

- Purpose: Provide clarity regarding research security program requirements, how research organizations will be expected to satisfy the requirements, and how agencies will contribute to program content development.

- Security program content (research organizations over $50M in federal funding for each of the previous 2 fiscal years)
  1. Cybersecurity
  2. Foreign travel security
  3. Research security training
  4. Export control training, as appropriate

5. Foreign Travel Security

- Research organization must maintain international travel policies including:
  - Organizational record of covered international training by faculty and staff (optional disclosure/authorization requirement in advance of training)
  - Security briefings
  - Electronic device security (smartphones, laptops)
  - Pre-registration requirements

5. Research Security & Export Controls

- Need research security point of contact (with contact info)
- Research organizations must provide training to relevant personnel on:
  - Research security threat awareness and identification
  - Consider incorporating research security into RCR
  - Conduct tailored training in the event of a security incident
- Export control training (as appropriate)
  - Train relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators, and partnerships
  - Ensuring compliance with export control requirements and restricted parties lists

5. Research security requirement

- Any additional security requirements beyond standard ones must be in the award terms and conditions
- OSTP, with NSTC Subcommittee, will issue standardized requirement for uniform implementation
  - 90 day external engagement period + 120 days to develop requirement and then work with OMB to implement
- Federal govt will provide standardized technical assistance to support development of training content and programmatic guidelines, tools, and best practices
- List of cybersecurity basic safeguarding principles are included in the guidance
- Research agencies should engage with external stakeholders to ensure that program requirements are appropriate to the broad range of organizations subject to the requirement

5. Research security requirement

- **Single organizational certification standard and process that applies across all research agencies will be developed (rather than a proposal-specific certification)**
- Organizations will need to maintain and provide descriptions of their research security programs within 30 days of an agency request
    - May become part of the Compliance Supplement
- Deadline to comply will be one year from date of issuance of the formal requirement (or one year after the organization becomes subject to the requirement)

Jim, Lori and Pamela also extend special thanks to …

- David Wright, FDP
- Sara Pietrzak, FDP

- Lynette Arias, U of Washington
- Robin Cyr, Northeastern University
- Kim Moreland, U of Wisconsin
- Susan Anderson, College of Charleston
- All the members of FDP Foreign Influence Group (FIWG)

A question

is

a

window.