February 28, 2022

Submitted via Email to Addresses below and to ResearchSecurity@ostp.eop.gov

Linda Lourie, Assistant Director for Research and Technology at Linda.S.Lourie@ostp.eop.gov
White House Office of Science and Technology Policy (OSTP)
Co-Chair, National Science and Technology Council Joint Committee on the Research Environment's Subcommittee on Research Security ("Subcommittee on Research Security")

Christina Ciocca Eller, Assistant Director for Evidence & Policy, OSTP at Christina.C.Eller@ostp.eop.gov
Co-Chair, Subcommittee on Research Security

RE: Listening Session Comments Concerning the January 2022 Guidance for Implementing NSPM-33

Dear Ms. Lourie and Dr. Eller:

The Federal Demonstration Partnership (FDP) is an association of federal agencies, academic research institutions with administrative, faculty and technical representation, and research policy organizations that work to streamline the administration of federally sponsored research. FDP members of all sectors cooperate in identifying, testing, and implementing new, more effective ways of managing the more than $15 Billion in federal research grants. The goal of improving the productivity of research without compromising its stewardship has benefits for the entire nation.

The FDP uniquely offers a forum for individuals from universities and nonprofits to work collaboratively with federal agency officials to improve the national research enterprise. At its regular meetings, faculty and administrators talk face-to-face with decision-makers from agencies that sponsor and regulate research. They hold spirited, frank discussions, identify problems, and develop action plans for change. Then – again working jointly – they test the new ways of doing things in the real world before putting them into effect.

Objective

The objective of the attached document is to identify those areas of the NSPM guidance where stakeholders seek clarification or wish to offer implementation ideas for consideration. This document was created for a number of Listening Sessions with the FDP Foreign Influence Working Group (FIWG) and partners from NSF (Jean Feldman & Rebecca Keiser), NIH (Michelle Bulls), DoD (Jason Day), and Energy (Steve Binkley & Helena Fu); these sessions were held on February 16th and 17th via zoom.

Preamble and Opening Comments

The Federal Demonstration Partnership (FDP), through its unique partnership between research institutions and federal representatives, has an impressive track record of collaborations. In support of this collaboration and the important elements of the NSPM-33 Guidance, we would like to first comment generally on a number of critical elements both in process and content related to the Guidance.

FDP appreciates:

a) your continued openness to input from the user community; FDP continues to stand ready and offer input throughout the process and coordinate sessions with diverse perspectives including from ERIs, HBCU's, smaller research institutions, etc. as well as collecting specific input from the faculty community.
b) your focus on Harmony, especially around terms and definitions; FDP's Research Terms and Conditions could be an applicable model for future deliberation: see https://www.nsf.gov/awards/managing/rtc.jsp
c) your openness to allowing research institutions to rely on their own policies; this flexibility will support the diversity in size and complexity of the breadth of the nation's research institutions
d) your selective and careful use of "Must" and "Should" in the development of the guidance
e) your policy development and implementation considerations that allow some flexibility and actively encourages participation in research from smaller grantees with limited resources as well as large research-intensive institutions
f) your emphasis and considered concern about not unintentionally promoting discrimination against foreign nationals; poor policy and/or implementation could have a harsher impact on the nation's research institute's if this is not kept at the forefront of this important initiative

In closing, the FDP will be holding several educational sessions for the membership; on March 24th at 3:00 pm we will focus on Digital Persistent Identifiers (DPIs) and in early April, we will have a joint federal and university panel to collectively advance the discussion on implementation.

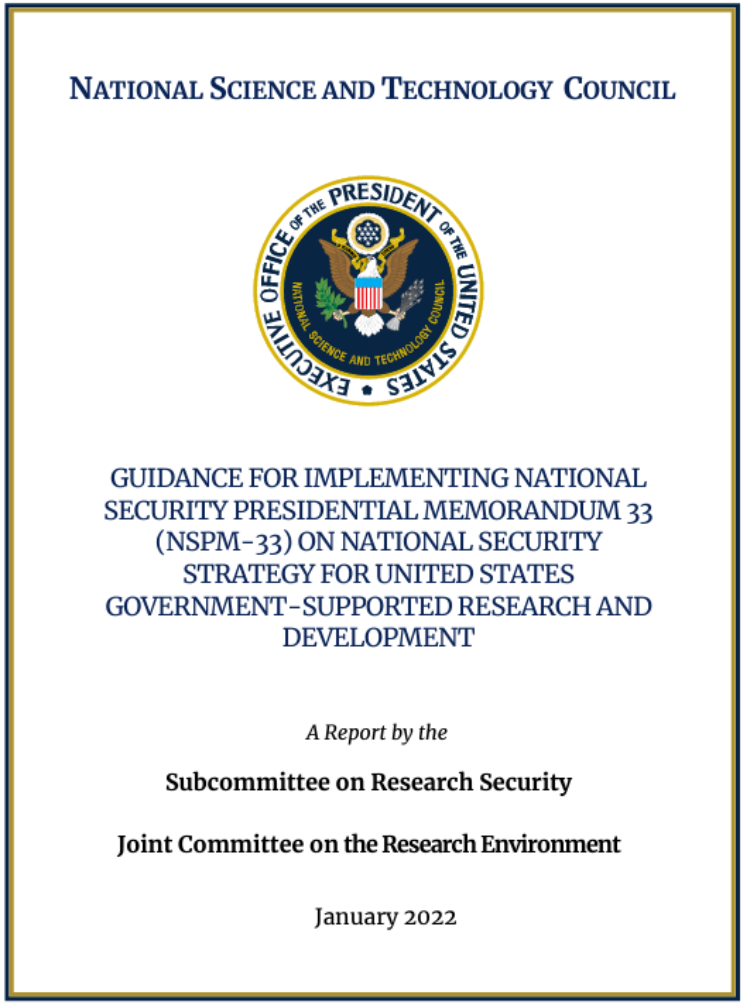
Alex Albinak (FDP Co-Chair)
Johns Hopkins University

Michele Masucci, Ph.D (FDP Co-Chair)
Temple University

Cc: Steve Binkley, DOE
Michelle Bulls, NIH
FDP Foreign Influence Working Group members
Jason Day, DOD
Jean Feldman, NSF
Helena Fu, DOE
Rebecca Keiser, NSF
Jim Luther, FDP
Pamela A. Webb, University of Minnesota

FEDERAL DEMONSTRATION PARTNERSHIP

Redefining the Government & University Research Partnership



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

FDP Evaluation and Feedback on NSPM-33 Implementation Guidance

Presenters:

Alex Albinak, Johns Hopkins University

Jim Luther, FDP

Michele Masucci, Temple University

Pamela Webb, University of Minnesota

OSTP Engagement Hours

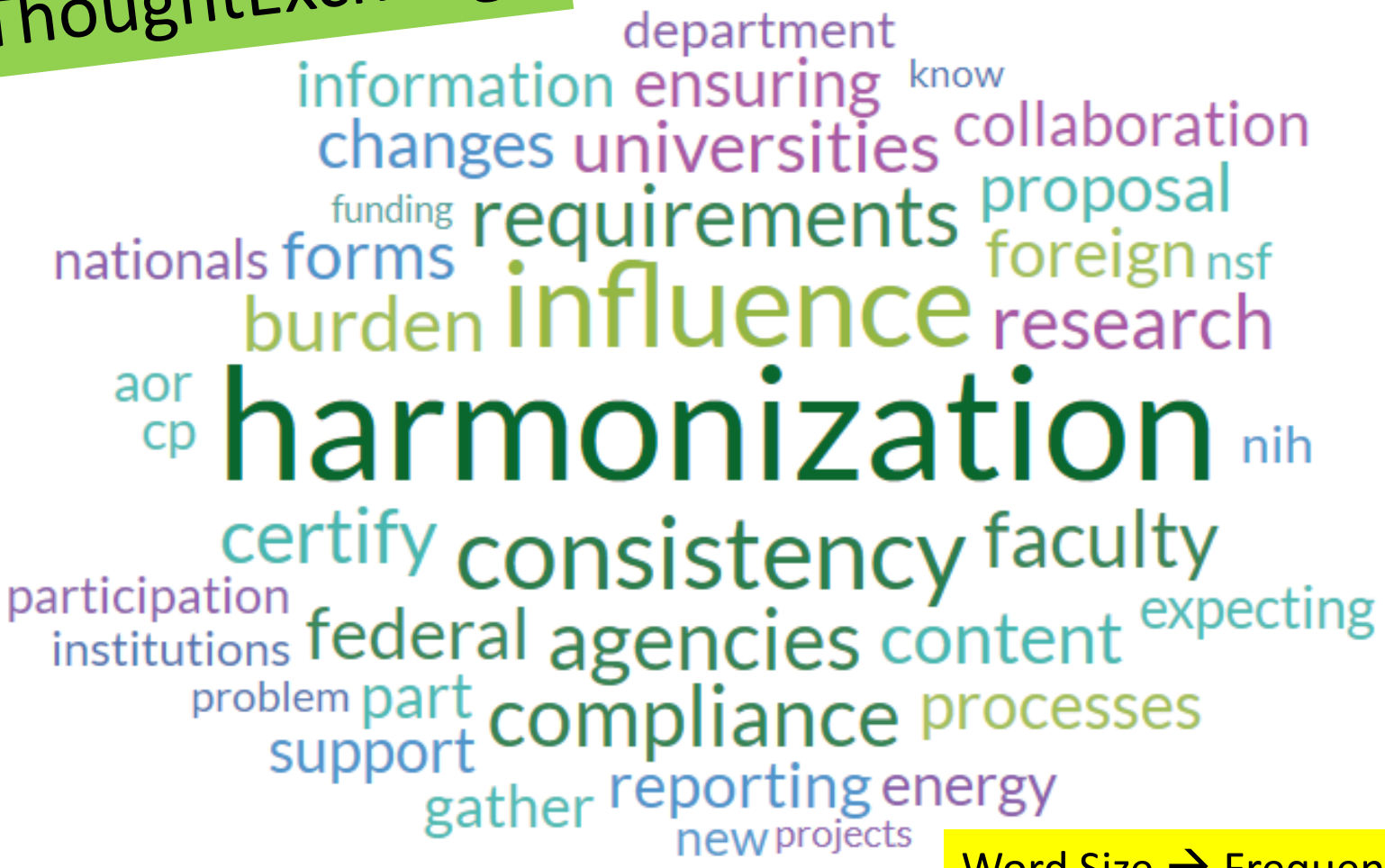
February 28, 2022

Description of FDP

- A cooperative initiative convened by the Government-University-Industry Research Roundtable (GUIRR) of the National Academies of Sciences, Engineering, and Medicine (NASEM).
- A unique forum for individuals from universities and nonprofits to work collaboratively with federal agency officials to improve the national research enterprise through identifying, testing and implementing new and effective ways of managing federal research awards.
- Started in 1986, currently includes 10 federal agencies and 217 organizations with representatives from university administration, faculty, and electronic research administration managers (organizations range from ERIs and HBCUs to multi-billion dollar institutions).
- Convenes and meets three (3) times a year: September, January, and May.

Areas of FDP Interest

ThoughtExchange



Word Size → Frequency
Word Color → Related Words

FDP Evaluation of NSPM-33 Implementation Guidance

- 5 working groups from FDP Foreign Influence Working Group (FIWG) involving faculty, technologists, and research administrators
- Identification of:
  - Areas needing additional clarity
  - Ideas for implementation
  - Definitions in need of more precision
- Listening Sessions (2/16 and 2/17) with federal agency representatives (NIH, NSF, DOD, DOE)
  - FDP FIWG *Evaluation of NSPM-33 Implementation Guidance* Discussion Document (distributed)

FDP Impressed with:

- Unequivocable commitment to non-discrimination and fair treatment for all members of the research community
- Strong commitment to build on excellent work on disclosures already done by NIH and NSF (already includes significant stakeholder input)
  - And willingness to continue the dialogue as expressed by NIH, NSF, DOD and DOE
- Willingness to create and share baseline content for research security training programs
  - And willingness to engage with research enterprise for jointly prepared training modules and tools

Important Clarifications Sought

- Broadly understood definitions of standardized terms will be essential to success – how can these best be optimized?
- What rigor and process will be used to evaluate agency-requested deviations from standardized requirements
- Who will be a "covered person" mandated to disclose?
  - Expansion would significantly impact administrative burden
- How will DPIs be incorporated into pre-award and post-award processes (now and planning for the future)?
- How, when and what potential disclosure violations will be shared across agencies prior to final findings or determinations?
  - Premature release can cause reputational harm for investigators and institutions that cannot easily be remedied

Clarifications (continued)

- What will be the process for identifying and assessing disclosure failures, and associated range of consequences and mitigating factors?
  - Recipients need detailed information regarding administrative remedy and enforcement processes
- How will “routine use” be expanded?
- What privacy rules will apply, and at what stage of these processes?
- What will be the respective roles and responsibilities of agencies, institutions, and investigators in assessing disclosure failures and consequences?

Clarifications (Continued)

- Additional details about research security requirements and expectations are needed
  - How will the $50M threshold for research security programs be deployed (particularly for subrecipients)
  - With respect to fundamental research, will there be cross-agency harmonized baselines for research security, foreign travel security, cybersecurity, and training?
  - How will institutions know which requirements apply, and to whom?
  - How will institutions learn of special research security threats, or insider threats (and how best to respond)
  - What are the expected requirements/responsibilities of the Research Security Point of Contact?

Implementation Ideas

- All agencies use the same definitions for standardized terms
  - Additional terms added where customization is needed
- Lead time is needed (for creation and roll-out of research security training, system changes, “catch-up” with evolving disclosure obligations)
- Require notification to investigators/institutions before sharing preliminary allegations or findings of disclosure violation (to allow for correction if needed)
- Create ombudsperson or advisory committee to allow for appeals or to correct overreach
- Use Federal Register ANPRMs or other mechanism to pre-validate final disclosure forms and requirements
  - Create future change management process that includes stakeholder input

Implementation Ideas (continued)

- Create incentives for use of DPIs
- Encourage strategic use of funding where needed to promulgate transformative change
  - Enhancements to SciENcv or to agency systems to accept data directly from DPI providers
- Harvest the power of the research enterprise (including FDP) to validate implementation roll-out and to develop and deploy training modules, tools and techniques
  - Just released NSF RFA for training module development is a great start!

FDP Next Steps

- March 24, 2022 (3 pm) FDP Webinar on "*Introduction to Digital Persistent Identifiers*"

- April 2022 (TBD) FDP broad-based Listening Session on NSPM Implementation Guidance
  - NIH, NSF, DOD and DOE have agreed to participate

- Definitional Clarity + engagements
  - Meetings between agency officials and FDP FIWG member to clarify definitions; may also be used for specialized feedback (e.g., small research institutions, faculty-specific feedback)


A question
is
a
window.

FDP Foreign Influence Working Group

Evaluation of NSPM-33 Implementation Guidance

Updated Working Copy as of 2-27-22

This document has been produced by institutional members of the Federal Demonstration Partnership (FDP). Started in 1986, the FDP currently includes 10 federal agencies and 217 diverse universities, colleges, and affiliated research organizations, and is convened by the Government-University-Industry Research Roundtable (GUIRR) of the National Academies of Sciences, Engineering, and Medicine (NASEM). FDP provides a unique forum for university administrators, faculty, and technologists to work collaborative with each other and with federal agency officials to improve the national research enterprise through identifying, testing, and implementing new and effective ways of managing federal research awards. More information about FDP can be found at thefdp.org.

The purpose of this document is to identify those areas of the NSPM guidance where FDP institutional stakeholders seek clarification or wish to offer implementation ideas for consideration. Input is organized to align to the five major sections of the NSPM implementation guidance document.

I. DISCLOSURE REQUIREMENTS AND STANDARDIZATION (WORK GROUP LEADS: AMANDA HUMPHREY AND ROBIN CYR, NORTHEASTERN UNIVERSITY)

Group: Amanda Humphrey, Robin Cyr, Lynette Arias, Laura McCabe, Doug Backman, Jim Luther

Clarifications sought

A. **The degree to which definitions will be required to be identical for the same term is unclear.** For clarity, training, and to reduce the probability of error or omission in disclosure, an identical term should be used the same way across all agencies. Additional terms can be added if an alternate meaning is intended. Certain terms, such as "outside activities" can appropriately be left to local discretion. How will consistency of terminology and definitions be achieved?

B. **The population of investigators required to disclose (or disclose under certain circumstances) appears to offer agencies considerable latitude for deviation for "*other compelling reasons consistent with individual agency authorities and as coordinated through the NSTC*" and/or for when "*variations to standards are warranted*."** What will be the process for determining when such a deviation is warranted?

C. **The degree to which NSTC will compel or coordinate harmonization of requirements across agencies is unclear.** What deviations can be expected to rise to the level of a "compelling reason consistent with individual agency authorities?" What checks and balances exist to ensure, especially over time, that deviations are necessary and appropriate?

D. **The definition of "covered individual" was expanded in NDAA 2021 Sec 223 (and repeated in the NSPM Implementation Guidance).** What is the intended purpose behind the change, and who else is intended to be included? Specifically, the new guidance defines a "covered

individual to be one who "contributes in a substantive, meaningful way" to the scientific development or execution of an R&D award, as opposed to the traditional term of someone who "is responsible for the design, conduct, or reporting". The "responsible for" element of this definition has historically been key.

E. **Consulting continues to be an area where additional clarification may yet be needed.** The FDP would welcome being able to work with federal partners to continue the excellent work undertaken by NIH and NSF on this important topic.

F. **Norms or standard scientific practices may eventually need to be updated/refined to harmonize with updated disclosure requirements** (e.g., the process by which author names are added to publications; mutual understanding of what arrangements constitute an "appointment" or an "affiliation" and mutual concurrence that it has been officially invoked. This is likely a longer-term improvement but should be noted.

G. **The respective roles and responsibilities of agencies, prime recipients, and subrecipients need to be defined in final implementation guidance.** For example, agencies should define whether subrecipients report disclosure errors directly to agencies or to their prime recipient. It should be made clear what actions each party is expected to take to obtain, review, or monitor requirements. A common approach adopted across the federal government for how this can best occur is preferred.

H. The new requirements to disclose Private Equity and Venture Capital financing need additional context and requirements. Definitions, roles and responsibilities in this space need additional clarification.

Implementation ideas

1. **Provide lead time for institutions to train investigators and administrators on new and refined definitions, to create and conduct training, and for systems and business processes to be updated.**

2. **Carefully assess any potential expansion of who must disclose beyond today's PI and senior/key personnel requirements.** Specifically, burden and benefit should be carefully assessed. For example, students and postdocs change frequently, are often hired immediately prior to project need, and are replaced throughout the project lifecycle. Visiting researchers come and go, and how these individuals are expected to disclose needs more clarity. Adding new categories of individuals who must disclose will slow science and add administrative burden.

3. **Consider use of of the FDP Key Investigator Clearinghouse ("KIC") and Matrix for Assessment of Risk and Transparency" (MART) concepts as implementation plans proceed.**

II. DIGITAL PERSISTENT IDENTIFIERS (WORK GROUP LEAD: LORI SCHULTZ, UNIVERSITY OF ARIZONA)

Group: Lori Schultz, Susan Anderson, Pamela Webb, Laura McCabe, Jim Luther

Clarifications sought

A. **The extent to which application/progress report processes will be affected by researcher certification/agency review of connected DPI information is unclear.** DPIs offer a wealth of opportunity for reduced administrative burden and improved precision of information but may result in major business process changes as well. Clarity around agency expectations (ideally with a commitment for considerable stakeholder input prior to finalization of processes) will assist with adoption.

B. **Relative to Section 4 of this document (Information Sharing), recipients are concerned that information could be shared prior to determination of guilt.** Recipients would like to understand how this information would be shared when it is accessed via a linked DPI, especially in relation to point-in-time accuracy of information.

C. **DPIs can potentially be deployed in the research context for more than just individuals.** In the short/medium term, will federal agencies require DPIs other than ones for individuals?

D. **DPIs could potentially be deployed at multiple time points in the grant life-cycle.** If DPIs are not required in the application process, will provisions be made for scenarios when a researcher obtains one later (during review, progress reporting, etc)?

Implementation ideas

1. **Define key terms in the DPI universe (see final section).**

2. **Standardize terms for reportable/disclosable items across agencies to maximize effective administrative burden reduction, and so that researchers have an understanding of how data in their DPI-connected profile will be interpreted by funding agencies.**

3. **Ensure consistent collection of the DPI at the application stage for all agencies and capture these in a form or requirement that is included in all agency application packages.** Possibilities include:
   a. SF424 Cover Page
   b. Harmonized biosketch form referenced in the OSTP guidance

4. **Define processes and key checkpoints for how DPI-connected information will be (a) Expected to be shared/certified by the researchers, and (b) accessed by the federal agency**

5. **Provide inherent incentives by planning for a future state where having a DPI provides the most benefit in reducing administrative burden.** For example, investigators with a DPI can make use of the flexible ecosystem, while those without will continue to use form sets.

6. **Define a workflow/process for researchers to include a DPI after the application process, possibly at Just-In-Time, or with a progress report.**

III. CONSEQUENCES FOR VIOLATION OF DISCLOSURE REQUIREMENTS (WORK GROUP LEAD: SHANDRA WHITE, NORTHWESTERN UNIVERSITY)

Group: Shandra White, Pam Caudill, Alice Young, Doug Backman

Clarifications sought

A. **Clarity is needed about when potential or applied consequences and administrative actions are directly related to noncompliance with disclosure requirements (e.g for other support) versus the content of the information that has been disclosed**. In addition, clarity on when consequences are applicable to an individual investigator versus when a consequence is applicable to the institution is needed. The implementation guidance is suggestive as to principles in this regard but more details would guide institutional implementation.

B. **Information about administrative remedy and enforcement processes is not known at this time. Recipients wish to have detailed information regarding these processes.** Who will decide if a violation has occurred and whether there are any mitigating factors? How and with whom (e.g., which agencies and institutions) would actions such as restrictions and ineligibility for participation on awards be shared? Would the restrictions be enforced inter-agency?

C. **It is anticipated that some individuals will need to come forward and correct past omissions.** More detail is requested on the impact of self-disclosure on any consequences and potential for remediation of participation restrictions.

Implementation ideas

1. **Invoke either a joint or lead agency approach in the event there needs to be cross-agency collaboration on a single investigator/single institution issue.** Either a joint or lead agency would be preferable to institutions needing to manage potentially different requests or requirements from multiple agencies on the same issue. It would be helpful to articulate how this process will occur.

2. **Publish detailed policies, procedures and timelines for required actions such as submitting corrections and remediation efforts.** Agency grant policy manuals should include detailed procedures for all required actions.

IV. INFORMATION SHARING (PAMELA WEBB, LEAD)

Group: Pamela Webb, Lori Schultz, Robin Cyr, Michele Masucci, Lynette Arias

Clarifications sought

A. Recipients have a major concern that sharing of information within or across agencies or with the public prior to a final determination of guilt can cause irreparable (and inappropriate) harm to investigators. Stakeholders need to be clearly informed about the circumstances under which such sharing should occur, what will be shared, and should be notified in advance**.** The list of examples you provide is encouraging.

B. Roles and responsibilities need to be defined (and any intended change in practice noted) between institutions, agencies and law enforcement with respect to disclosure investigations. Recipients worry that they will be expected to play a more explicit role as an arm of law enforcement or that there may be an expectation that universities share new information with law enforcement that they have not historically been asked to or been expected to provide. Examples of such information include local assessments of risk or in-progress investigative details. Institutions may not be legally able to disclose this information, nor may it be appropriate to do so.

C. Clarification is needed about what constitutes a "routine use" in existing systems of records and the due process for agencies developing new routine uses that could result in agencies sharing information related to violations and potential violations.

D. Recipients need to be informed about what constitutes an "administrative action" and whether it includes just agency administrative actions or both agency and institutional administrative actions. Institutions may not be legally able to disclose this information, especially related to an in-progress investigation

E. What is included in due process, privacy considerations, and "consistent with applicable laws, regulations, and policy"? What protections are provided at what points in the processes. Recipients need to have this information to be able to inform investigators and to be able to comment if needed.

F. What will be the timing of the "research agencies" implementing updated disclosure obligations? Will there be a phase-in period, to afford time to ensure faculty understanding and respond to their questions about historical and current relationships, collaborations, affiliations, and sources of foreign support?

Implementation ideas

1. **Create an ombudsman and associated adjudication panel to hear and address recipient concerns** (e.g. about information being shared prematurely or more broadly than permitted

under law or policy) To ensure objectivity, we suggest that a panel include non-conflicted parties (agencies, IGs, and stakeholder representatives.)

2. **Provide notifications to investigators and their institutions if information is going to be shared among agencies or with the public, including the specifics about what will be shared**, the basis for the belief for that information, and allow for a factual correction period prior to release.

3. **Deploy a matrix (such as COGR's Appendix I on Information Sharing (p. 7 of their Summary) to aid training/understanding related to information sharing and privacy rights**

4. **Deploy phase-in period to allow time for training and review of existing relationships and support that may need to be disclosed**. Acknowledge that requirements represent a major change for investigators and allow for "safe" reporting of past relationships that didn't previously require disclosure

V. RESEARCH SECURITY PROGRAMS (WORK GROUP LEAD: PAMELA CAUDILL, YALE UNIVERSITY)

Group: Pam Caudill, Lori Schultz, Jim Luther, Michele Masucci, Laura McCabe, Mark Sweet

Clarifications sought

A. **Define how the $50M threshold will be determined, published, and how recipients need to use that information for organizations beyond their own (e.g., subrecipients).** How will institutions know if others meet the threshold? Should this be stipulated in SAM? [Note: For ~300 organizations, this could be easily added to in the FDP Expanded Clearinghouse]

B. **It is unclear how new cybersecurity requirements will align with the upcoming DOD security requirements (NIST 800-53), and the extent to which they will apply across the portfolio of work performed (including for systems that are used in performance of award activities outside of the applicant organization's oversight.)**

C. **Clarification is needed on the timing of cybersecurity reuirements (all within one year?) and cost allowability (direct charge, allowable part of a service center, or indirect)**. It was noted that these costs were never contemplated at the time the F&A administrative cap was set in 1991.

D. **For foreign travel security, the definition of what is intended by "as appropriate" and "covered international travel" in the context of a disclosure and authorization requirement in advance of travel is unclear.** Does it matter who is paying for the travel, or only if required under the terms of the award, or only if there is classified or CU information? Does it include student travel (including travel to their home country?)

E. For foreign travel security, what is the expectation for electronic device security? Specific guidance would be appreciated.

F. **Significant clarification is needed in terms of expectations for Research Security training.** Institutions need to have a better understanding of the universe of concerns to ensure that content is appropriate, understanding government-provided or government mandated content versus optional or institution-supplied content, acceptable modality (in-person or on-line, including in RCR or not), and a better understanding of the required audience.

G. Clarification is needed about what additional research security training is expected "In the event of a research security incident"

H. It is unclear how recipients would be expected to know about a specific research security threat? Is research threat awareness the same as insider threats, and is it specific to the research context?

I. How can FDP be included in the Community Consortium? How will faculty/investigators be included in the collaborative effort?

J. Export control training is required "as appropriate". Is this intended to mean subject to export control restrictions? How to speak to institutional training versus faculty training? Knowledge of law? Institutional policy?

K. What are the requirements/responsibilities of the Research Security Point of Contact? (Can or should this person be the same as the individual who manages classified or CUI? Is the PoC expected to be responsible for training and tracking of training? Are there requirements for authority and responsibility?

Implementation ideas

1. **Accommodate various size entities and types of research portfolios in your research security requirements.**

2. **Define baseline cybersecurity targeted to educational institutions.**

3. **Require baseline harmonization across agencies (eg., for baseline requirements).** Additional requirements should be risk-based and associated with well-defined thresholds or markers (e.g., work being performed is classified or includes CUI)

4. **Ensure that stakeholders have the opportunity to review any proposed guidelines sufficiently early in the process that changes can still be made to ensure the requirements are clear and achievable.**

5. **Use existing federal databases (e.g. SAM) wherever possible to help with clarity** (e.g., is an institution subject to research security program requirements)

6. **Deploy easily accessed links to location-specific guidance for foreign travel security;** an easily accessed link to location specific guidance would be helpful.

VI. DEFINITIONS

During the course of our evaluation, the need for clear, unambiguous definition of terms, harmonized across agencies (with different terms being deployed when a different meaning is needed) was a recurring theme. Terms needing to be defined include the following:

[NOTE: AS OF 2/14/22, THIS SECTION IS A WORK IN PROGRESS AND THE FULL LIST WILL BE PROVIDED AT A LATER TIME; EXAMPLES ARE PROVIDED BELOW FOR THE TYPE OF INFORMATION INTENDED TO BE LISTED]

1. **COVERED INTERNATIONAL TRAVEL.** The "covered" aspect of this needs to be defined. Does it matter who is paying for the travel or whether it is directly related to the research being performed under a project? Is this invoked only under certain circumstances (e.g., if there is classified or CUI information?) Does it include student travel (including travel to their home country?)

2. **DIGITAL PERSISTENT IDENTIFIER (DPIs).** DPIs, also known as Persistent Identifiers (PIDs) are unique IDs used to represent a person, organization, scholarly output, among other things, including grants and contracts awarded by federal agencies. DPIs/PIDs are expected to be Digital (machine readable and actionable, i.e., findable on the internet), Unique (to the thing they reference), and Persistent (long-lasting link to the person, place, or object). The OSTP guidance refers only to DPIs for individuals, but reducing burden will necessitate use of other DPIs.

3. **INSIDER THREAT.** The term "insider threat" is often used to indicate risk to an organization's operations or systems from persons inside, or formerly from, the institution. How will this definition (and required training) apply when threats are from outside the organization (other organizations or possible collaborators), and may differ from threats related to classified or controlled unclassified information?