COGR

Council On Governmental Relations

An Association of Research Institutions

Summary of NSTC Guidance for Implementing National Security Presidential Memorandum 33: Provisions Regarding DPIs, Consequences, Information Sharing and Research Security Programs

On January 14, 2021, the White House issued "Presidential Memorandum on United States Government – Research and Development National Security Policy" (NSPM-33"). NSPM-33 tasked the heads of U.S. research funding agencies with establishing policies on various aspects of research security, including:

- Researcher disclosure requirements
- Use of digital persistent identifiers (DPIs)
- Appropriate consequences for disclosure violations
- Sharing of information about violators, as consistent with applicable laws
- Standards for research security programs

In August 2021, the Office of Science and Technology Policy (OSTP) announced that it would produce guidance for research funding agencies in implementing NSPM-33 to promote harmonization among agencies' policies in this area to the extent possible and practicable. This long-awaited guidance -- "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development" (hereafter the "NSPM-33 Guidance") -- was issued on January 4, 2022, by OSTP acting through the National Science and Technology Council (NSTC) Joint Committee on the Research Environment (JCORE) Subcommittee on Research Security.

COGR previously issued a document summarizing the NSPM-33 Guidance key points regarding disclosure requirements, which can be found on the COGR website. This summary highlights key points of the NSPM-33 Guidance that address the other topics covered by the document: DPIs, consequences, information sharing, and research security programs.

Key Points Regarding DPIs

- **Background**: A persistent identifier is a unique identifier that permanently identifies a digital object on the internet. Unlike many URLs, which often contain broken links as they age, a persistent identifier is managed to provide consistent and continuous access to a digital object. These persistent identifiers may be used to identify a contributor to a scholarly work and can be used to resolve any confusion regarding contributors to a work by disambiguating among authors with the same or similar names. An ORCID ID (Open Researcher and Contributor Identifier) is one example of a digital persistent identifier or

DPI. [*See*, U.S. Dept. of Transp., Nat'l Transp. Library Guide, Persistent Identifiers; ORCID, "What are persistent identifiers (PIDs)"].

Over the past few years, several research funding agencies have compared the results of literature reviews with information contained in disclosures made to the agency and used this information to identify affiliations or resources that an individual researcher may not have disclosed. Such searches may result in false positives if they are conducted using identifiers that may be potentially ambiguous (e.g., common names). The use of DPIs can help reduce such ambiguity. Additionally, if services that provide DPIs are consistently used, individuals can employ these services to maintain, in one place, a complete and up-to-date record of their scholarly achievements. The NSPM-33 recognized this potential use of DPIs and gave funding agencies a year to establish policies on requirements for researchers to register with a DPI service. The NSPM-33 Guidance constitutes a first step on this path by providing instruction to agencies on incorporating DPIs into application/disclosure processes and setting forth core standards that DPI services used for disclosures should meet.

- **Option to Use DPIs in Funding Application and Disclosure Processes**: The NSPM-33 Guidance advises research funding agencies that they should permit the submission of required disclosures via a DPI service (e.g., ORCID) and outlines a potential process that researchers could follow if such a service is used. In short, the researcher would establish/maintain a profile in the DPI service that includes all disclosures required by the funding agency and certify to its completeness and accuracy. When disclosures are required in connection with a funding application, the researcher would then give the funding agency permission to access the profile, thereby eliminating the need to enter data into more than one system. Notably, the researcher would have the *option* to use the DPI service for this purpose, but per the NSPM-33 Guidance, agencies also should permit application processing without a DPI service.

- **Standards for DPI Services:** The NSPM-33 Guidance encourages agencies, if possible, to utilize/leverage existing DPI services provided by private vendors that are widely used by researchers. The Guidance provides several key parameters agencies should require of DPI services used for disclosure purposes, including: enable creation of single CV-type record, allow researcher information to be transmitted to agencies and awardee institutions, enable use of information from multiple systems, integrate with standard authentication services, and be free of cost to researchers.

    - **Privacy**: One key standard is that researchers be able to control access to their information on file with the DPI service by setting privacy levels and specifying those entities that may access their information. Further, the NSPM-33 Guidance states that agencies should not require researchers to provide public disclosure via the DPI service.

Key Points Regarding Consequences for Violations

- **Background:** NSPM-33 requires research funding agencies to ensure that they have appropriate and effective consequences for disclosure requirement violations and "engagement in other activities that threaten research security and integrity." Consequences may include civil, criminal, or administrative sanctions/actions, and the NSPM-33 Guidance reminds agencies that potential criminal violations should be thoroughly investigated by inspector generals (IGs) or referred to appropriate units of the Department of Justice.

- **Liability of Research Organizations and Potential Consequences**: The NSPM-33 Guidance references the provisions of Section 223 of the FY 2021 National Defense Authorization Act ("Section 223"). Section 223 limits the use of certain "enforcement" actions listed in Section 223(c)(2) against a research entity to the following circumstances:

    - Entity fails to make an individual employed by the entity, and listed on the award application, aware that the individual must disclose amount/type/source of all current and pending research support; certify that the disclosure is accurate and complete; and agree to update such disclosure prior to any award, and as otherwise requested by the funding agency; or
    - Entity knew that the individual failed to disclose the required information and did not take any steps to remedy the situation before a funding application was submitted; or
    - The head of the research agency determines that the entity is owned/controlled/substantially influenced by the individual and the individual failed to disclose the required information. [Section 223(c)(3)].

  Importantly, the NSPM-33 Guidance does not consider all the actions listed in Section 223(a)(2) to be "enforcement" actions and it draws a distinction between "enforcement administrative actions and remedies" that can only be taken against research institutions if the foregoing criteria are met and "non-enforcement administrative actions and remedies" that may be taken against research institutions without meeting the foregoing criteria. Notably, it appears that one action -- whole or partial suspension/termination of a federal award – is listed in the NSPM-33 Guidance as both an "enforcement" and "non-enforcement" administrative action/remedy. [*Compare* NSPM-33 Guidance, Paragraph 2, p. 11-12 and Paragraph 7, p. 13 (including Table 3 listed thereunder)]. There may be potential arguments that (a) all actions listed under Section 223(c)(2) should be considered "enforcement" actions and/or (b) that the NSPM-33 Guidance itself considers all items listed under Paragraph 2, p. 11-12 as "enforcement' actions. However, it is unclear whether Section 223 was intended to limit the government's ability to terminate an award under 2 CFR §200.340 for non-compliance. COGR will attempt to seek clarification on this issue. **Table 1** below lists those administrative actions/remedies that the Guidance classifies as (a) enforcement administrative actions and remedies and (b) non-enforcement administrative actions and remedies and notes in red the enforcement action/remedy that the NSPM-33 Guidance appears to include in both categories. Items highlighted in yellow are those items that appear in NSPM-33 Guidance, Paragraph 2, p. 11-12.

Table 1: Potential Consequences for Violations Detailed in NSPM-33 Guidance

Enforcement Administrative Actions and Remedies		**Non-Enforcement Administrative Actions and Remedies**	
Remedy	**Source**	**Remedy/Monitoring**	**Source**
Non-procurement debarment & suspension (i.e., ineligibility to participate in government programs)	2 CFR Part 180 and agency specific regulations	Federal agency risk review of applicant and adjustment of award requirements based on evaluation	2 CFR § 200.206
Procurement debarment, suspension, & ineligibility of contractors	48 CFR Part 9, Subpart 9.4, and agency specific regulations	• **Remedies:** ◦Imposition of specific conditions on federal award (e.g., payments. as reimbursements; approval to proceed to next phase on provision of evidence of acceptable performance; additional/more detailed financial reports; additional project monitoring; technical/mgmt. assistance; additional prior approvals). ◦Withhold cash payments pending correction of deficiency; disallow all/partial costs; wholly/partially suspend/terminate award; withhold further federal awards for project/program). • **Monitoring/admin. actions:** Financial and performance reports; site visits; video conferences, calls, emails.	2 CFR § 200.208 (Specific Conditions) 2 CFR § 200.339 (Remedies for Noncompliance) 2 CFR § 200.340 & .341 (Termination & Notification of Termination) 2 CFR § 200.329 (Monitoring & Reporting Program Performance)
Additional administrative actions potentially available to agencies (e.g., rejection of R&D award application; preserve R&D award but require/ensure that individuals don't perform work under the award; ineligibility for participation in U.S. government review panels and other activities; suspension/termination of federal employment; suspension/termination of R&D award; placement of individual or research organization in FAPIIS)	Agency-specific regulations		
Dept. of Education termination, suspension, or limitation of participation in Higher Education Act (HEA) Title IV programs if non-disclosure violates HEA §117	20 USC §1011f		

- **Transparency of Process and Factors Agencies Should Consider in Determining Sanctions**: The NSPM-33 Guidance instructs agencies to clearly document enforcement and administrative remedy processes, and the NSTC will prepare a standard operating procedure in this regard that agencies may use. The Guidance also lists factors agencies should consider in determining what consequences to impose, including: harm caused; intent; offender's knowledge of requirements; single or multiple violations; existence/timing of self-disclosure; policies/processes/training available to offender; and any other mitigating factors.

- **Processes for Self-Disclosure and Correction**: Agencies are charged with "encouraging self-disclosure and correction" of disclosure omissions/errors, as well ensuring that mechanisms for correcting disclosure errors are straightforward and clearly communicated (including any timetables). Agencies should consider self-disclosure favorably in administrative resolution of nondisclosure issues.

Key Points Regarding Information Sharing

- **Background:** NSPM-33 directed heads of agencies to share information with each other and with law enforcement agencies about individuals who violate disclosure requirements, participate in foreign government-sponsored talent programs (FGSTP) in violation of law/policy, or take part in activities that "clearly demonstrate an intent to threaten research security and integrity," provided that such sharing is consistent with applicable law. The NSPM-33 Guidance calls on agencies to be clear as to when they will share information and to detail how they will limit sharing to respect privacy and to ensure due process. The chart in **Appendix 1** below summarizes the NSPM-33 Guidance instruction to agencies about circumstances when information should be shared and mechanisms for sharing. Note that the NSPM-33 Guidance makes clear that agencies should share information "consistent with due process, privacy considerations, and all other applicable laws."

Key Points Regarding Research Security Programs:

- **Background**: NSPM-33 requires that by January 14, 2022, funding agencies require research institutions that receive more than $50 million per year in "Federal science and engineering support" to certify that the institution operates a research security program.
- **Institutional Qualification**: The funding threshold for the research security program requirement will be calculated based on the funding received by an institution during the two prior fiscal years as set forth in USASpending.gov.
- **Content of the Research Security Program**: Programs must include elements of cyber security, foreign travel security, insider threat awareness, and, as appropriate, export control training. The NSPM-33 Guidance provides additional details about each of these elements, which are summarized in the chart included as **Appendix 2** below. A baseline research security program including these elements will be required for all research organizations that meet the funding threshold.
- **Classified Research or Research Involving CUI**: Organizations that conduct classified research or research involving controlled unclassified information (CUI) must meet the

more stringent security requirements for those types of research, as well as the broader NSPM-33 Guidance requirements. Agencies should not mandate classified or CUI research security requirements for fundamental research. If research funding agencies require additional security elements for certain types of non-classified/non-CUI research (e.g., research on emerging/critical technology with implications for U.S. national/economic security) then such requirements should be included in award terms and conditions.

- **Development of Research Security Program Content and Stakeholder Input**: OSTP, in consultation with NSTC, OMB, and external stakeholders, will develop standard program requirements for "uniform implementation across research agencies." The federal government will provide technical assistance in the development of training content and program guidance that research organizations may use, but agencies should provide institutions with flexibility to structure their research security program to meet individual circumstances and to leverage existing programs. The NSPM-33 Guidance suggests that the government consider supporting the formation of a "community consortium to develop and maintain research security program information and implementation resources for research organizations." Notably, the Guidance states that the development of program content should be "a collaborative effort between the government and organizations" to the greatest extent possible.
- **Timeline and Certification/Documentation Requirements:**
    - **Timeline for Federal Government Development of Program Content:**
        - 90-day period for government to engage with community stakeholders
        - 120-day content development period after conclusion of engagement period
        - After agencies receive the standardized program content, they should further engage with stakeholders regarding appropriateness of standards.
    - **Timeline for Institutional Compliance:** Institutions will have one year from the date that a formal requirement to comply is issued by which to establish a research security program.
        - **Institutional Compliance Certification**: Institutions will be required to provide certification of compliance with the research security program requirement. OSTP, in consultation with NSTC and OMB, will establish a single certification standard and process to be used across funding agencies, as opposed to integrating certification into the award application process.
        - **Documentation Requirements**: Institutions will be required to maintain documentation of their research security program and provide the documentation to a federal funding agency within 30 days of an agency request.

Point of Contact for Additional Information:

For additional information or questions regarding this summary document, please contact Kris West, Director Research Ethics & Compliance at kwest@cogr.edu.

Appendix 1: Summary of NSPM-33 Guidance on Information Sharing

	Share with Other Funding Agencies	Share with Law Enforcement	Share with Public	Sharing Mechanism
Potential Violation[1]	• When potentially relevant to other research agency mgmt. of federal R&D funding (e.g., undisclosed affiliation with foreign research org.; undisclosed funding; indication of duplicative funding to single PI; identical proposals from one or more PIs, when one or more is funded by another agency). • In support of risk analysis/analytics to understand scope/scale of research security challenge, particularly when steps are taken to reduce risk of re-identifying individuals.	• When referring to an appropriate law enforcement entity for further investigation or consideration of enforcement/admin. action. • Inspector General (IG) must report to Atty. General when IG has reasonable grounds to believe there is violation of federal criminal law. • IG and FBI must mutually notify each other in all matters involving fraud against federal government.	• Whenever feasible, share results of risk analyses, particularly when steps are taken to reduce risk of re-identifying individuals. Do this to promote transparency and promote public understanding of research security risks and consequences of violations.	• Via routine uses outlined in agency Privacy Act notices. • Via legally established law enforcement reporting channels. (See examples under "Share with Law Enforcement.")
Violation[2] Finally Determined	• When potentially relevant to other research agency mgmt. of federal R&D funding. (See examples above for sharing a Potential Violation.) • In support of risk analysis and lessons learned, particularly when steps are taken to reduce risk of re-identifying individuals.		• Whenever feasible, share results of enforcement processes to promote transparency and promote public understanding of research security risks and consequences of violations.	• SAM.gov – gov.-wide exclusions such as suspension or debarment, voluntary exclusions. • FAPIIS – notify agencies re. criminal, civil, and admin. proceedings in connection with awards, including admin. agreements in lieu of suspension/debarment and award terminations for default, cause, or material failure to comply.
Administrative or Enforcement Action Taken	• Sharing and public notification as required by enforcement action (e.g., record suspension/debarment in SAM.gov).		• Whenever feasible, share results of administrative remedy and enforcement processes to promote transparency and public understanding of risks/consequences.	See Sharing Mechanisms for "Violation Finally Determined."

[1] ***Potential Violation***: *A situation that merits further investigation by appropriate authorities to determine if a violation of a requirement has occurred.*
[2] ***Violation***: *Determination through a criminal, civil, or administrative process that a violation of a requirement has occurred.*

Appendix 2 Research Security Program Components

	General	Cyber Security	Foreign Travel	Research Security Trg.	Export Controls
Specific Elements	**Point of Contact**: Designated research security point of contact (POC). (May be the same as the POC for classified research or research using CUI.)	**Training**: Regular cybersecurity awareness training for authorized users of information systems, including recognition/response to social engineering threats and cyber breaches.	**Policy:** International travel policy for faculty/staff traveling for organization business, teaching, conference attendance, or sponsored travel "that would put a person at risk."	**Insider Threat**: Threat awareness and identification, including insider threat awareness where applicable	**Training on Processes for Foreign Collaborations:** Institutions that conduct R&D subject to export control restrictions should provide training to relevant personnel on requirements/process for reviewing foreign sponsors, collaborators, and partnerships.
	Contact for POC: Publicly accessible method for contacting the POC (e.g., website, social media).	**Limit Access to Systems**: Limit information system access to authorized users/devices	**Travel Record:** •Organization record of covered international travel. •Pre-registration requirements	**Periodic & Event Specific Training:** Periodically provide general training and consider tailored training in the event of a security incident.	**Training on Export Control Requirements**: Training for ensuring compliance with federal export control requirements and restricted entities lists.
		Limit Function Access: Limit information system access to transactions/functions permitted for authorized users	**Disclosure/Approval Process:** Advance disclosure and/or authorization of international travel (as appropriate).	**Incorporation into RCR Training**: Consider incorporating elements of research security training into responsible and ethical conduct of research training for faculty/students.	
		Limit Connections: Verify, control, limit connections to/use of external information systems.	**Security briefings**		

	General	Cyber Security	Foreign Travel	Research Security Trg.	Export Controls
		Non-Public Information: Control non-public information posted/processed on publicly accessible information systems	**Device Security:** Assistance with electronic device security		
		Identification/Authentication: Identify information system users, processes, devices and authenticate identities before allowing access.			
		Monitor and Protect Communications: Monitor, control, and protect organizational communications at external and key internal boundaries of information systems.			
		Subnetworks: Implement subnetworks for publicly accessible system components that are physical/logically separate from internal networks			
		Data Integrity: Protect scientific data from ransomware and data integrity attack mechanisms.			
		Correct Flaws and Implement Updates: Identify, report, and correct information system flaws in a timely manner, and update malicious code protection mechanisms when new releases are available.			
		Malicious Code Protection: Provide protection from malicious code at appropriate locations in information systems.			
		System and File Scans: Perform period scans of information systems and real-time scans of files from external sources when they are downloaded, opened, or executed.			