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

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at http://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at http://www.whitehouse.gov/ostp.

About the Subcommittee on Research Security

The Subcommittee on Research Security is an interagency group organized under the NSTC Joint Committee on the Research Environment (JCORE). The purpose of the Subcommittee on Research Security is to coordinate Federal Government efforts to enhance the security and integrity of America's science and technology research enterprise without compromising American values or the openness of the innovation ecosystem. The Subcommittee is focused on coordinating appropriate and effective risk management, coordinating Federal efforts to effectively communicate and provide outreach to academic and research organizations, developing guidance for agencies on security and integrity of the Federally-funded research enterprise, and developing recommended practices for academic and research organizations.

About this Document

The purpose of this document is to provide guidance to Federal departments and agencies regarding their implementation of National Security Presidential Memorandum 33 on National Security Strategy for U.S. Government-Supported Research and Development.

Copyright Information

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL [AS OF DECEMBER 2021]

Chair

Eric Lander, Director, OSTP

Acting Executive Director

Kei Koizumi, Principal Deputy Director for Policy, OSTP

JOINT COMMITTEE ON THE RESEARCH ENVIRONMENT

Co-Chairs

Geraldine Richmond, Under Secretary for Science and Energy, Department of Energy

Eric Lander, Director, Office of Science and Technology Policy

Francis Collins, Director, National Institutes of Health

James Olthoff, Performing the Duties of Under Secretary of Commerce for Standards and Technology and Director, National Institute of Standards and Technology

Sethuraman Panchanathan, Director, National Science Foundation

SUBCOMMITTEE ON RESEARCH SECURITY

Co-Chairs

Steve Binkley, Department of Energy

Rebecca Keiser, National Science Foundation

Mike Lauer, National Institutes of Health

Linda Lourie, Office of Science and Technology Policy [from June 2021]

Christina Ciocca Eller, Office of Science and Technology Policy [from October 2021]

Aaron Miles, Office of Science and Technology Policy [through September 2021]

Members

Department of Agriculture
Department of Defense
Department of Education
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation
Federal Bureau of Investigation
Food and Drug Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology
National Institutes of Health
National Oceanic and Atmospheric Administration
National Science Foundation
National Security Agency
National Security Council staff
Office of the Director of National Intelligence
Office of Management and Budget
Office of Science and Technology Policy
United States Geological Survey
United States Patent and Trademark Office

Significant contributors to this work also include Ryan Donohue, OSTP.

Table of Contents

Abbreviations and Acronyms

CFR Code of Federal Regulations

DPI digital persistent identifier

FY fiscal year

HEA Higher Education Act

NDAA National Defense Authorization Act

NSPM National Security Presidential Memorandum

NSTC National Science and Technology Council

OIG Office of the Inspector General

PI principal investigator

R&D research and development

U.S.C. United States Code

Foreword by NSTC Chair Eric Lander

One of America's most amazing and enviable superpowers is that we are the leading magnet for talented scientists and engineers from around the world. They come to study, to found startups, to lend their energies to U.S. scientific and technology endeavors, to start research labs, and to build ties between cultures, communities, and countries — and they become incredible members of our scientific community. For instance, of this year's four American winners of the scientific Nobel Prizes, three immigrated to the United States.

The research security challenges we face are real and serious: some foreign governments, including China's government, are working hard to illicitly acquire our most advanced technologies. This is unacceptable.

At the same time, if our policies to address those actions significantly diminish our superpower of attracting global scientific talent — or if they fuel xenophobia against Asian Americans — we will have done more damage to ourselves than any competitor or adversary could. So we need a thoughtful and effective approach.

In August, I announced that the White House Office of Science and Technology Policy (OSTP) would work through the National Science and Technology Council to develop the implementation guidance for National Security Presidential Memorandum-33, with the goal of providing clear and effective rules for ensuring research security and researcher responsibilities.

This implementation guidance is a product of close collaboration across the federal government, and I am immensely grateful to everyone who contributed to it — in OSTP, in fellow Cabinet departments and other federal agencies, and in the wider Executive Office of the President. I am equally grateful to the researchers and research institutions who provided vital perspectives that helped inform this effort.

The implementation guidance reflects the principles I laid out in August: to protect America's security and openness, to be clear so that well-intentioned researchers can easily and properly comply, and to ensure that policies do not fuel xenophobia or prejudice. But there is more work ahead to fulfill these important goals.

As a next step, I am now directing federal research 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 research funding agency. The goal is for the government to clearly describe what it needs to know and for researchers to be able to report the same information in the same way to the greatest extent possible, regardless of which funding agency they're applying to. Clearly laying out the required information will ease administrative burdens on the research community, and it will also enable software developers to make tools to enable researchers to populate digital CVs from which they can readily export relevant information.

While current efforts on NSPM-33 seek to clarify and simplify how researchers disclose information to the federal government, they do not address other key questions about NSPM-33 implementation — namely, how the government uses this information in making decisions about research funding and support. Such questions are equally important, and OSTP intends to address them in the future. Where the government has legitimate concerns about a potential conflict of interest or conflict of commitment, we have a responsibility to be clear and open about what our concerns are and why. It is important to avoid undue, vague, and implicit pressures on researchers, as this could create a chilling atmosphere that would only constrain and damage the U.S. scientific enterprise.

The Biden-Harris Administration is strongly committed to both protecting research security and maintaining the core ideals behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values. As we do so, we will continue to engage with the remarkable and diverse community of U.S. researchers and institutions, who enable so much of our country's scientific progress.

Dr. Eric S. Lander
Assistant to the President for Science and Technology
Director, White House Office of Science and Technology Policy

Vision for Our Shared Research Environment

Since World War II, America's research enterprise has been second to none, and it has delivered profound benefits for our health, economy, and national security. This leadership has been rooted in the core commitment of our shared research environment to openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

Some foreign governments, including those of the People's Republic of China, Russia, and Iran, are working vigorously in violation of these values to acquire, through both licit and illicit means, U.S. research and technology. There have been efforts to induce American scientists to secretively conduct research programs on behalf of foreign governments or to inappropriately disclose non-public results from research funded by U.S. Government sources. This is unacceptable.

Preventing such abuses is a shared responsibility. It requires clear commitment, transparency, and communication from not only the Federal Government but also from research organizations and individual researchers. The Biden-Harris Administration envisions a shared research environment that both protects research security and maintains the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

Activities To Date

During its final week in office, the previous administration issued a National Security Presidential Memorandum (NSPM-33) to "strengthen protections of United States Government-supported R&D against foreign government interference and exploitation" while "maintaining an open environment to foster research discoveries and innovation that benefit our nation and the world."

On August 10, 2021, the White House Office of Science and Technology Policy committed to developing clear and effective implementation guidance for NSPM-33, and tasked the National Science and Technology Council to lead that process. This report contains guidance that represents the first step towards implementing NSPM-33 effectively, rigorously, and uniformly across the Federal Government in a way that protects the nation's interests in both security and openness.

The Office of Science and Technology Policy is grateful for the time and effort that colleagues in the National Security Council staff, fellow Cabinet agencies, and other Federal agencies have invested through the National Science and Technology Council to develop this guidance, and for all the effort still to come to ensure that implementation of NSPM-33 does not overburden researchers or make it difficult for them to comply with relevant U.S. laws and regulations.

Although this guidance document is primarily intended to aid federal research agencies in harmonizing processes, the research community will be equally engaged in understanding and complying with the implications of this guidance.

A core principle of this guidance is that compliance with NSPM-33 and relevant laws and regulations must be as easy and uncomplicated as possible for the research community, particularly

as it pertains to the disclosure process. Transparently disclosing all relevant activities and information that bear on potential conflicts of interest and commitment is part of the broader set of researchers' responsibilities to ensure objectivity, honesty, transparency, fairness, accountability, and stewardship. Standardized disclosure requirements across agencies are expected to reduce uncertainty and establish clear, persistent guidelines for researchers to follow. Tools such as electronic curricula vitae (CVs), or digital persistent identifier (DPI) services, provide platforms that can facilitate easy compliance through persistent, easily accessible reporting tools. We encourage creators of DPI services to include all the categories of information that will be important for identifying—and avoiding—financial conflicts of interest and conflicts of commitment. From our perspective, we are not looking to favor one solution over another; we simply want all such solutions to meet the needs of both researchers and agencies.

It is also appropriate that consequences failing to disclose requested information—administrative, civil, or criminal penalties—should also be made clear.

Finally, it is essential that the policies and consequences must be applied without discrimination in any way, including with respect to national origin or identity.

Next Steps

The task ahead is to realize this vision. The work will include developing, within the next 120 days, model award proposal disclosure forms and instructions to make clear what is expected of researchers. The goal of these standardized forms and accompanying instructions is to ensure that applying for awards from any Federal research funding agency will require disclosing the same information in the same manner, to increase clarity and reduce administrative burden on the research community. (In some cases, research agencies may adapt the forms and instructions, where required by their legal authorities.) Such model forms will also allow the research community to identify and point out where greater clarity may be needed. They can also provide clarity to developers building electronic CVs and other tools to help streamline the processes for disclosure.

The work also will include further efforts by this Subcommittee to develop common standards for research security program requirements for use by Federal agencies, as well as a standard and centralized research security program certification process for use by research organizations.

Everyone involved in the research enterprise, including the U.S. Government, research organizations, and researchers, has a role in both protecting research security and maintaining the core values that drive American leadership in science, technology and innovation: openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

Introduction to Implementation Guidance

National Security Presidential Memorandum 33 (NSPM-33) established national security policy for U.S. Government-supported R&D. The purpose of NSPM-33 is to strengthen protections of U.S. Government-supported R&D against foreign government interference and misappropriation, while maintaining an open environment to foster research discoveries and innovation that benefit the United States and the world.

As Federal departments and agencies ("agencies") work to implement NSPM-33, it is critical that they do so in a consistent, coordinated manner that preserves the open and collaborative nature of the U.S. research enterprise, while providing strong and effective measures to protect research security and reinforce adherence to research responsibilities, transparency, and equity.

The purpose of this document is to provide guidance to Federal departments and agencies regarding their implementation of NSPM-33. The guidance does not create or confer any rights for or on any person or entity and does not operate to bind any department or agency of the U.S. Government or the public. It includes general guidance that agencies should apply across their implementation efforts, followed by more detailed guidance in five key areas addressed in NSPM-33:

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

Consistent with NSPM-33, this guidance includes a significant focus on upholding transparency through clearly-articulated requirements and processes for appropriate disclosure of information related to potential conflicts of interest and conflicts of commitment. Effective implementation of research security policy will make it more difficult for individuals to conceal materially important support, obligations, conflicts of interest, and/or relationships that, when concealed, could lead to Federal research agencies ("research agencies") making inadequately informed funding decisions. Effective implementation will also make it easier for R&D award[1] recipients and research agencies to identify and address noncompliance in a timely and fair manner.

In addition, agencies should note that this document does not provide budget guidance. The allocation of funding related to activities described in this document should follow regular agency budgetary processes. This implementation guidance is subject to the Office of Management and Budget's budgetary, legislative and administrative processes and nothing in this document should be construed to imply support in future budgets.

[1] See Definitions Appendix. For the purposes of this report, R&D awards include grants, cooperative agreements, contracts, and other transactions. The guidance provided herein pertains to individuals applying for R&D awards, unless otherwise indicated.

General Implementation Guidance

The following general guidance applies across NSPM-33 implementation activities.

- Agencies should continue to support open and transparent scientific inquiry.
- Agencies should coordinate together, through the National Science and Technology Council (NSTC), to ensure that implementation of NSPM-33 is uniform across agencies, to the greatest extent practicable. Agencies should avoid taking major NSPM-33 implementation actions, including but not limited to new regulations, requirements, and disclosure forms, unless coordinated through the NSTC. Disclosure forms should advise that false representations may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§287, 1001, 1031 and 31 U.S.C. §§3729-3733 and 3802.
- Agencies should integrate implementation of NSPM-33 requirements with implementation of applicable statutes, including Sec. 223 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2021 and Section 117 of the Higher Education Act (HEA) of 1965, as amended.
- Agencies should provide clear instructions, jointly and separately, on how research organizations can satisfy the applicable NSPM-33 requirements. Approaches to implementation should avoid imposing excessive administrative burden on researchers, research organizations, and agencies, while ensuring compliance with the NSPM-33 requirements.
- 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.
- Agencies should incorporate measures that are risk-based, in the sense that they provide meaningful contributions to addressing identified risks to research security and integrity and offer tangible benefit that justifies any accompanying cost or burden.
- When introducing changes to regulations, policies, and procedures, agencies should avoid retroactive application that would unnecessarily harm researchers currently supported by Federal funding.

Unlike the prior points, which represent guidance, the following point is a requirement authorized by NSPM-33:

- Agencies 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.

Disclosure Requirements and Standardization

Background: Section 4(b) of NSPM-33 directs that "*research funding agencies shall require the disclosure of information related to potential conflicts of interest and commitment from participants in the Federally funded R&D enterprise… The appropriate disclosure requirement varies depending on the individual's role in the United States R&D enterprise.*" Section 4(b)(vi) directs that "*agencies should standardize forms for initial disclosures as well as annual updates, … and should provide clear instructions to accompany these forms and to minimize any associated administrative burden.*"

Objective: Provide clarity regarding disclosure requirements (e.g., who discloses what, relevant limitations and exclusions), disclosure process (e.g., updates, corrections, certification, and provision of supporting documentation), and expected degree of cross-agency uniformity.

Implementation Guidance

1. *Standardization of disclosure requirements*

Disclosure requirements will be standardized across research agencies to the greatest extent practicable. Variations among research agencies should be limited to cases (a) where required by statute or regulation; (b) where more stringent protections are necessary for protection of R&D that is classified, export-controlled, or otherwise legally protected; or (c) for other compelling reasons consistent with individual agency authorities and as coordinated through the NSTC.

The disclosure of information indicated in Table 1 will be required across all research agencies, in accordance with the role of the participant in the R&D enterprise. More details on types of activities to be disclosed by Tier I[2] individuals are listed in Tables 2a and 2b.

Table 1. General NSPM-33 disclosure requirements for Tier I and Tier II participants.

Disclosures Required From:	Organizational Affiliations/ Employment	Positions/ Appointments	Foreign gov.-sponsored talent recruitment programs[3]	Current and pending support/ Other Support
Tier I • **Principal investigators (PIs) and other senior/key personnel** • **Program officers** • **Intramural researchers[4]**	**Y**	**Y**	**Y**	**Y**
Tier II • **Peer reviewers** • **Advisory committee/Panel members**	**Y**	**Y**	**Y**	**N**

[2] Tier I individuals are principal investigators and other senior/key personnel, program officers, or intramural researchers. Tier II individuals are peer reviewers and advisory committee and/or panel members (Table 1).
[3] See Definitions Appendix at the end of this report.
[4] See Definitions Appendix at the end of this report.

2. *Standardization of 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. The NSTC Subcommittee on Research Security will coordinate with NSTC member agencies, including the Office of Management and Budget (OMB), and with other relevant NSTC bodies to develop templates for updated biographical sketch forms and current and pending support forms, leveraging existing forms where possible, that are suitable for adoption across research agencies as standard forms. These forms also will include standard language for designating covered individuals as defined in Section 223 of the NDAA for FY 2021.

3. *Requirements for peer reviewer and advisory committee member disclosure of affiliations and positions*

Research agencies should require that peer reviewers disclose affiliations and positions. Research agencies should require that advisory committee and panel members disclose affiliations and positions only as they may relate to agenda items at each meeting, and pursuant to Office of Government Ethics approved processes. The NSTC Subcommittee on Research Security will coordinate with other relevant NSTC bodies to develop templates for standardized disclosure forms, and accompanying instructions for determining when affiliations and positions meet these conditions.

4. *Potential broadening of disclosure requirement to include students*

Standardized disclosure requirements for R&D awards are limited to covered individuals as defined in Section 223 of the NDAA for FY 2021, and other individuals explicitly identified in NSPM-33. Research agencies should not generally require disclosures from broader classes of individuals (e.g., graduate students, undergraduates), except when variations to standards are warranted, i.e., as identified in subsection 1 of this section.

5. *Collection of information associated with the required Tier I disclosure requirements within R&D award application processes (including pre-award and post-award elements[5])*

Research agencies have made significant progress in recent years towards establishing greater uniformity in R&D award application processes and associated disclosure requirements. Where practicable, research agencies should implement application processes and requirements in a manner consistent with the tables below, which leverage existing progress and provide consistency with NSPM-33 and Section 223 of the NDAA for FY 2021.

[5] As described in Title 2 of the Code of Federal Regulations (CFR) Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

Table 2a. Guidance for disclosure of personal and professional information within R&D award application processes.

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)		✓	✓	✓
Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs[6]	✓ (Appropriate placement may be contract-dependent)			
In-kind contributions not intended for use on the project/proposal being proposed		✓	✓	✓
Visiting scholars funded by an entity other than own institution		✓	✓	✓
Students and postdoctoral researchers funded by an entity other than own institution		✓	✓	✓
Travel supported/paid by an entity other than own institution to perform research activities with an associated time commitment		✓	✓	✓
Certification by the individual that the information disclosed is accurate, current, and complete		✓	✓	✓

[#]Some agencies may collect this information in Collaborators and Other Affiliations.

[6] See Definitions Appendix at the end of this report.

Table 2b. Guidance for disclosure of project information.

Type of Activity to be Disclosed	Facilities and Other Resources	Other
PROJECT INFORMATION		
In-kind contributions that support the research activity for use on the project/proposal being proposed	✓	
Private equity, Venture, or other capital financing*		✓
Supporting Documentation (e.g., contracts, grants, other agreements)^		✓

*See implementation guidance point 6 below.
^See implementation guidance point 11 below.

6. *Collection of information related to financial conflicts of interest within R&D award application processes*

Research agencies should require that recipient organizations instruct covered individuals on how to disclose information related to potential financial conflicts of interest, including but not limited to: private equity, venture, or other capital financing. If required by law or policy, covered individuals must provide these disclosures to both the research agency and to the organization applying for or receiving the Federal funding. Policies at some other research agencies require that covered individuals provide conflict of interest disclosures only to the organization applying for or receiving the Federal funding.

7. *Exclusions from disclosure requirements within R&D award application processes*

Research agencies should exclude the following information from research agency disclosure requirements, except under the conditions identified in Subsection 1 of this section:

- Completed support, including recently completed support
- Consulting that is permitted by an individual's appointment and consistent with the proposing organization's "Outside Activities" policies and procedures.[7]
- Honoraria (see Appendix for definition)
- Gifts (see Appendix for definition)
- Mentoring as part of appointment
- Teaching commitments at the recipient organization
- Academic or calendar year salary earned at the recipient organization

8. *Clarification regarding exclusion of gifts from disclosure requirements*

Compensation or consideration that are provided with terms and conditions and in support of R&D activities are not considered gifts 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), and do not require disclosure except when required by Section 117 of the HEA, as amended.

[7] Notwithstanding any exclusion from research agency disclosure requirements, research organizations typically require disclosure of paid consulting for consideration of potential financial conflicts of interest. 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. Authorship or co-authorship on a scientific or technical published paper or posted pre-print would be one manifestation of an activity that involves research.

9. Requirements for disclosing core facilities and shared equipment

Research agencies should require disclosure of resources available to the specific researcher, such as additional research space or personnel, but should generally not require disclosure of institutional resources that are made broadly available to faculty and staff, except where necessary to evaluate the viability of the proposal.

10. Requirements for disclosing participation in foreign programs

The specific requirement to disclose participation in, or application to, programs sponsored by foreign governments, instrumentalities, or entities is limited to those that are associated directly or indirectly with a foreign government (i.e., foreign governments or foreign government instrumentalities or entities). However, participation in foreign programs that are not directly or indirectly associated with a foreign government will in many cases still be captured under other disclosure requirements, such as affiliations, appointments, and other support.

11. Requirements for disclosure of foreign contracts to research agencies

Consistent with NSPM-33, research agencies will require that individuals disclose contracts associated with participation in programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs,[8] upon request of the recipient research organization or the research agency. Some research agencies may choose to incorporate this request as a standard required element of their R&D award application process. Research agencies also may require disclosure of a broader range of contracts pertaining to foreign activities, beyond those associated with participation in foreign government-sponsored programs (e.g., contracts, grants, and all other agreements for foreign participation, whether or not sponsored by a foreign government). Non-disclosure clauses associated with these contracts are not acceptable exemptions from this disclosure requirement.

12. Just-in-time submission of application information

Research agencies may choose whether to require a "just-in-time" submission—meaning after the completion of peer review but prior to funding—of R&D award application information. Consistent use of digital persistent identifiers across research agencies, as described in the next section of this guidance, will reduce any administrative burden associated with differing agency approaches.

13. Requirements for updating disclosures after an award has been made

Research agencies will require initial disclosures and updates to disclosure reporting. Updates should occur prior to the award of support, annually, more frequently, or promptly where the research agency deems appropriate to account for individuals' changing circumstances and for additions of covered individuals to funded research teams. For example, research agencies might require certified updates as part of post-award reporting or as a condition of receipt of a final tranche of funding to ensure current, accurate, and complete information is provided.

[8] Many countries sponsor talent recruitment programs to attract researchers in targeted fields. Many programs utilize legitimate, transparent mechanisms of talent recruitment, including use of research fellowships, student and scholar exchanges, and grants. However, some programs provide direction or levy requirements, including through language in binding contracts, that create conflicts of interest and/or conflicts of commitment for researchers; some have been shown to encourage or direct unethical and even criminal behaviors.

14. Process(es) for individuals to correct inaccurate or incomplete submissions

Research agencies will ensure that mechanisms for correcting disclosures exist, are communicated clearly, and are simple and straightforward. Research agencies should develop and implement both pre- and post-award processes, and consistent standard award terms and conditions, that enable PIs and other senior/key personnel and/or their organization to correct inaccurate and/or incomplete submissions.

15. Requirements and processes for research organizations applying for R&D awards to provide certification related to disclosure requirements

Research agencies will require certification by the applicant organization that each covered individual who is listed on the application has been made aware of all relevant disclosure requirements, including the requirements of Section 223 of the NDAA for FY 2021, and should advise that false representations may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§287, 1001, 1031 and 31 U.S.C. §§ 3729-3733 and 3802. The NSTC Subcommittee on Research Security will draft standardized language for potential adoption by research agencies and by which organizations could provide this certification.

Digital Persistent Identifiers

Background: Section 4(b)(v) of NSPM-33 directs that "*Consistent with applicable Federal laws and statutory authorities, within 1 year of the date of this memorandum, funding agencies shall 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.*" Section 4(b)(vi) directs, in part, that "*agencies should standardize forms for initial disclosures as well as annual updates, integrating digital persistent identifiers wherever appropriate and practicable….*"

Objective: Describe how research agencies will incorporate digital persistent identifiers (DPIs)—also known as Persistent Identifiers (PIDs)—into disclosure processes to bolster research security and integrity while reducing administrative burden.

Implementation Guidance

Research agencies should work to implement DPIs into their electronic systems and processes as quickly as is feasible with appropriate protections for personally identifiable information. Until that time, completion of required disclosures using previous systems and processes may still be required. When available, the DPI option will facilitate population of this information into the requisite format.

1. Incorporation of DPIs into grant and cooperative agreement[9] application and disclosure processes

Research agencies should allow submission of required disclosure information via a DPI service, consistent with the Paperwork Reduction Act and the Privacy Act of 1974, as applicable. Basic process steps should include the following:

- Researcher maintains information required under cross-agency disclosure requirements on an individual "profile" or "record" maintained by a DPI service and associated with a DPI.
- During the grant application process, the individual provides their DPI and, via the DPI service, authenticates their DPI and authorizes the research agency to access the required information. This replaces any need for the researcher to manually enter the required disclosure information.
- As part of the grant application process, the researcher certifies to the research agency that the information disclosed through the service is current, complete, and accurate.
- In cases where there remain variations between research agencies' application processes (i.e., timing of certain disclosure, use of different collection forms), the impact of these differences on the applicant will be minimized. The DPI profile or record will contain the needed disclosure information and can be accessed by the research agency at the appropriate time, once the researcher has provided authorization.

[9] The DPI section pertains to individuals applying for grants or cooperative agreements. As indicated in point 3 of this section, agencies should consider providing a DPI option for other types of R&D award applicants.

- In cases where a research agency requires an additional disclosure that exceeds the standardized requirements, researchers may also be able to maintain the additional disclosure information on the DPI service, and similarly provide it to the research agency, as an alternative to providing such information separately to the requesting research agency.
- When annual or other updates are required, the researcher may simply ensure that the profile/record information is current, provide an updated authentication if needed for the research agency to access the updated information, and provide an updated certification regarding the completeness and accuracy of the information.

2. *Requiring DPIs versus providing as an option for disclosures*

All research agencies should provide the option of using a DPI service for disclosure, but also may retain the option for a grant or cooperative agreement application to be processed without the use of such a service. The DPI option should provide the lowest administrative burden for researchers, research organizations, and research agencies. Some research agencies currently require use of DPIs under some circumstances, and more may choose to do so.

3. *Categories of individuals provided a DPI option for disclosures*

Research agencies should provide the DPI option for all individuals seeking or receiving Federal R&D grant and cooperative agreement funding. Research agencies also should consider providing a DPI option for extramural researchers funded through non-grant mechanisms (e.g., contracts), and for intramural researchers.

4. *Use of available DPI services*

To the greatest extent possible, research agencies should leverage DPI services provided by private entities, including, where possible, services already widely used by researchers. Research agencies should coordinate to establish DPI service requirements, and may allow research organizations and/or researchers to utilize any service that meets those requirements. Research agencies should increase consistency and further reduce administrative burden by ensuring that one or more common DPI service is available for use across agencies. If multiple DPI services are used, agencies should develop processes to integrate information from DPI services to assess completeness and consistency. Use of multiple DPI services may increase administrative complexity and cost, potentially impacting data quality.

5. *Common/core standards that a DPI service should meet to be included as an option for disclosure in Federal grant and cooperative agreement application processes*

- Provided by an open, non-proprietary, researcher-driven platform, interoperable with the ISO 17729 certified global standard number service for identifying contributors to creative works including researchers, inventors, and authors.
- Disambiguates one researcher from another, distinguishing individual researchers from others with the same or similar name and allowing Federal research agencies to uniquely identify researchers included in government systems. The DPI service should ensure disambiguation by allowing the researcher to include all associated name variations and additional information that can ensure unique identification.

- Enables a researcher to create a single record that represents their curriculum vitae with relevant information (employment, education, funding, research outputs, etc.) to share with funders, publishers, researchers, and other organizations.
- Prevents unintentional creation of duplicate DPI records for the same researcher. In cases of unintentional duplicate DPIs, the service should allow for the identification and consolidation of records into a single DPI record for the researcher.
- Allows collection of disclosure information in a DPI record, reduces administrative burden by entering information once, and allows researcher information to be transmitted to research agencies and grant recipient organizations, as appropriate and as authorized.
- Provides an ability to exchange and make use of information from multiple systems.
- Supports connection between DPI-associated information about the researcher over time and is inclusive of researcher name changes or different name formats.
- Allows research agencies to read and write validated information associated with the DPI.
- Supports secure integration with standard authentication services, such as Security Assertion Markup Language (SAML) and Open Authentication (OAuth).
- Provided at no cost to the researcher.
- Allows the researcher to control access to the information, with the privacy level set by the individual researcher, specifically identifying the entities allowed to access the information.

6. *Ensuring interoperability across multiple options for DPI service*

DPIs that meet the common/core standards will allow for interoperability. To ensure that research agencies can support multiple interoperable DPI options, DPI services should be open, non-proprietary, and provide the ability to exchange information. If using multiple DPI services, agencies should develop processes to integrate information access services to ensure complete and accurate reporting of disclosure information provided via DPI services.

7. *Potential for public disclosure of information provided to research agencies via a DPI service*

Research agencies should not require that individuals provide any public disclosure through the DPI service. Researchers may choose to make information publicly available through their DPI profile or record. Agencies may choose to include DPIs in public records in support of open science activities and/or requirements.

Consequences for Violation of Disclosure Requirements

Background: Section 4(b)(ix) of NSPM-33 directs that *"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 in some cases, such as when individuals intentionally provide incomplete or incorrect information in the grant funding process, or misappropriate trade secrets or export controlled information. Federal agencies should consult with their Inspectors General, General Counsel, security officers, and/or law enforcement agencies as appropriate, to avoid compromising ongoing investigative and law enforcement activities..."*

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

Implementation Guidance

1. *Consequences for violation of disclosure requirements*

Violation of disclosure requirements may lead to criminal, civil, and/or administrative consequences as may be deemed appropriate based upon the particular facts of the violation. Violations should be thoroughly investigated by the cognizant IGs and referred to criminal and/or civil offices within the Department of Justice, when warranted. Such matters should also be referred to the agency if consideration of administrative actions is deemed appropriate. Such administrative actions may include suspension and debarment of individuals or research organizations, where consistent with 2 CFR § 180 and 48 CFR Part 9.4, and appropriate to protect the integrity of government grant and contract programs.

In addition to suspension and procedures set forth in 2 CFR § 180 and 48 CFR Part 9.4, a research agency may consider action pursuant to other authorities, including but not limited to:

- 2 CFR § 200.206 Federal awarding agency review of risk posed by applicants;
- 2 CFR § 200.208 Specific conditions;
- 2 CFR § 200.339 Remedies for noncompliance**;**
- 2 CFR § 200.340 Termination; and
- 2 CFR § 200.341 Notification of termination requirement.

While retaining appropriate flexibility to determine consequences for violations of disclosure requirements, agencies should consider a common set of factors, where relevant and consistent with applicable laws and regulation, and communicate such factors to the research community.

2. *Other potential administrative actions available to research agencies to address noncompliance with disclosure requirements*

Depending on the facts surrounding the violation, and consistent with due process requirements, research agencies may consider a range of actions, including upon recommendation of the cognizant OIG. Such actions include, but are not limited to:

- Rejection of an R&D award application;

- Preserving an R&D award, but requiring or otherwise ensuring that individual(s) do not perform work under the award;
- Ineligibility for participation in U.S. Government review panels and other activities;
- Suspension or termination of Federal employment;
- Suspension or termination of an R&D award;
- Suspension or denial of Title IV funds by the Department of Education; and
- Placement of the individual or research organization in the System for Award Management or Federal Awardee Performance and Integrity Information System to alert other agencies.

3. *Factors for consideration in determining appropriate administrative actions and other consequences*

Specific considerations apply to some regulatory administrative actions, and are set out in those regulations, along with administrative due process to which the subject of the action is entitled. Regarding other administrative and enforcement actions, agencies may include the following considerations, where relevant and consistent with applicable laws and regulations, in determining appropriate consequences for violations of disclosure requirements:

- Harm or potential harm to the agency, the Federal Government, U.S. taxpayers, and other National interests;
- Intent of the offender;
- The offender's knowledge of requirements;
- Pattern of violation versus isolated incident;
- Existing and timing of self-disclosure;
- Policies, procedures, and training available to the offender; and
- Any other mitigating factors

4. *Provision of more detailed information regarding administrative remedy and enforcement processes*

Agencies should document procedures, including roles and responsibilities, for addressing failures to disclose required information. The NSTC Subcommittee on Research Security will develop a standard operating procedure template by which research agencies can address, consistent with applicable laws and regulations, possible noncompliance with disclosure requirements on the part of covered individuals and research organizations.

5. *Encouraging individuals to come forward and correct past omissions*

Agencies will ensure that mechanisms for correcting disclosures exist, are communicated clearly, specify timeframes, and are simple and straightforward to the greatest extent practicable. Agencies should strongly encourage self-disclosure and correction of omissions and inaccuracies, including by ensuring that self-disclosure will be taken into consideration during the process of administrative resolution of noncompliance with disclosure requirements, and by publicly highlighting circumstances or instances where this occurs, where appropriate.

6. *Notice and due process in agency consideration and application of regulatory administrative action*

In accordance with Section 223 of the NDAA for FY 2021, a research agency that intends to take action for failure to comply with disclosure requirements shall, as appropriate and practicable, and in accordance with applicable laws and regulations, notify each individual or research organization subject to such action about the specific reason for the action, and shall provide such individuals and entities with the opportunity to, and a process by which, to contest the proposed action.

7. *Circumstances for potential imposition of consequences on research organizations*

In accordance with Section 223 of the NDAA for FY 2021, an administrative remedy or enforcement action, including those listed in Subsection 2 of this section, may be taken by a research agency against a research organization only in cases in which (a) the organization did not meet requirements for entities to certify that covered individuals have been made aware of disclosure requirements; (b) the organization knew that a covered individual failed to disclose required information and the research organization did not take steps to remedy such nondisclosure before the application was submitted; or (c) the head of the research agency concerned determines that the organization is owned, controlled, or substantially influenced by a covered individual; and such individual knowingly failed to disclose required information.

Where applicable, research agencies may apply other non-enforcement administrative actions and remedies to research organizations for noncompliance with disclosure requirements, including those recommended by the cognizant OIG, and including but not limited to those listed in the table below.

Table 3. Examples of non-enforcement administrative actions and remedies that may apply to research organizations for noncompliance with disclosure requirements.

Category	Examples	Citation
Monitoring/ administrative actions	• Financial and performance reports • Site visits • Video conferences, telephone calls, e-mails	2 CFR §200.329, Monitoring and reporting program performance
Remedies for noncompliance	• Specific award conditions • Require payments as reimbursements rather than in advance • Withhold authority to proceed to next phase pending evidence of acceptable performance within a given performance period • Require additional, more detailed financial reports • Require additional project monitoring • Require the organization to obtain technical or management assistance • Establish additional prior approvals	2 CFR §200.208, Specific conditions.
	• Withhold cash payments pending correction of the deficiency • Disallow all or part of the cost of the activity/action not in compliance • Wholly or partly suspend or terminate the Federal award • Withhold further Federal awards for the project or program	2 CFR §200.339, Remedies for noncompliance

8. *Circumstances for potential suspension or denial of Higher Education Act (HEA) Title IV funds*

Termination, suspension, or limitation by the Department of Education of an institution's participation in HEA Title IV programs (which would result in the denial of Federal student financial aid to its students) may be appropriate in cases where a failure to disclose foreign gifts or contracts constitutes a violation of a requirement under the HEA (e.g., HEA Section 117 disclosure requirements). Any proposed action under this provision must comply with the HEA's requirements for notice and opportunity of a hearing. Failure to meet disclosure requirements under other authorities (e.g., Section 223 of the NDAA for 2021) would not be subject to the remedies under the HEA.

Information Sharing

Background: Section 4(e) of NSPM-33 directs that "*To strengthen the effectiveness of response measures, heads of agencies shall share information about violators (e.g., those who violate disclosure or other policies promulgated pursuant to this memorandum, participate in foreign government-sponsored talent recruitment programs contrary to policies issued pursuant to section 4(c)(ii), or whose activities clearly demonstrate an intent to threaten research security and integrity) across Federal funding institutions and with Federal law enforcement agencies, the DHS, and State, to the extent that such sharing is consistent with privacy laws and other legal restrictions, and does not interfere with law enforcement or intelligence activities. Where appropriate and consistent with due process, privacy considerations, and all other applicable law, heads of agencies should consider providing notice to other Federal funding institutions in cases where significant concerns have arisen but a final determination has not yet been made.*"

Objective: Provide clarity regarding circumstances when agencies may share information regarding violations and potential violations,[10] and provide assurance regarding how such sharing will be limited to respect privacy and other legal and reasonable protections.

Implementation Guidance

1. *Circumstances for research agency sharing with other agencies information about violations of disclosure requirements*

Research agencies should share information about violations of disclosure requirements, consistent with due process, privacy considerations, and all other applicable laws:

- Where potentially relevant to other research agency management of Federal R&D funding. Examples include when a research agency identifies:
  - That a covered individual has an undisclosed affiliation with a foreign research organization and is also funded by other research agencies.
  - That a covered individual has undisclosed funding from another research agency, including indication of undisclosed duplicative funding (overlapping funding to a single PI).
  - Identical proposals from one or more PIs, where one or more is funded by other research agencies.
- Once an administrative or enforcement action is taken.
  - Notification is required for some actions. For example, suspension or debarment determination is recorded in the System for Award Management (SAM.gov).
- In support of risk analysis and lessons learned, particularly where agencies have taken steps to reduce the risk of re-identifying individuals, to the greatest extent practicable.

[10] In this context, a "violation" may be established through a criminal, civil, or administrative process; a "potential violation" merits further investigation by appropriate authorities.

2. *Circumstances for appropriate research agency sharing of information prior to final determination of a violation*

Research agencies should share information with other agencies prior to a final determination of a violation in the following circumstances, consistent with due process, privacy considerations, and all other applicable law:

- Where potentially relevant to other research agency management of Federal R&D funding. This includes indications of the example circumstances listed in Subsection 1 of this section.
- 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/analytics to better understand scope and scale of research security challenges, particularly where agencies have taken steps to reduce the risk of re-identifying individuals, to the greatest extent practicable.

3. *Mechanisms for research agency sharing of information regarding violations with each other and with the public*

Mechanisms for research agency sharing of information regarding violations related to research security and integrity include the following:

- Agencies use the System for Award Management website (SAM.gov) as the information sharing mechanism for government-wide exclusions (e.g. suspension or debarment), including voluntary exclusions, issued in response to violations.
- Agencies use the Federal Awardee Performance and Integrity Information System (FAPIIS) to notify other agencies regarding actions including, but not limited to: criminal, civil, and administrative proceedings in connection with Federal awards; administrative agreements issued in lieu of suspension or debarment; and award terminations for default, for cause, and for material failure to comply.
- Agencies may publish mandatory and agency-level exclusions in SAM.gov under the Prohibition/Restriction section, on the Federal Register, and/or agency websites.
- Whenever feasible, agencies should seek to publicly share information about results of risk analyses and administrative remedy and enforcement processes to maximize transparency and enhance public understanding of research security risks and the consequences of confirmed violations.

4. *Mechanisms for research agency sharing of information regarding potential violations*

IGs are required to report expeditiously to the Attorney General whenever the IG has reasonable grounds to believe there has been a violation of Federal criminal law [Section 4(d) of the Inspector General Act of 1978, as amended (IG Act)]. The Attorney General Guidelines for OIGs with statutory law enforcement pursuant to Section 6(e)(4) of the IG Act requires OIGs and the Federal Bureau of Investigation mutually to notify each other in all matters involving fraud against the Federal Government. OIGs may coordinate with other law enforcement agencies on a need-to-know basis consistent with their respective routine uses for investigative records.

In addition to leveraging existing mechanisms where appropriate, research agencies should coordinate to establish improved mechanisms for sharing information among research agencies and their program offices.

5. *Proper sharing of information about violations and potential violations*

Agencies will ensure that sharing of information about violations and potential violations is appropriate and consistent with applicable laws, regulations, and policy. Agencies will work with their senior agency officials for privacy to ensure compliance with applicable privacy requirements in statute, regulation, and policy, such as those related to the Privacy Act of 1974. Agencies will evaluate the extent to which routine uses identified in existing system of records notices sufficiently address information sharing associated with research security and, where necessary, develop new routine uses for relevant research agencies to share with each other information related to violations and potential violations of disclosure requirements.

Research Security Programs

Background: Section 4(g) of NSPM-33 directs that by January 14, 2022, "*heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. Heads of funding agencies shall consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.*"

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

Implementation Guidance

1. Requirements for research security programs

NSPM-33 requires a certification from research organizations awarded in excess of $50 million per year in total Federal research funding that they have implemented a research security program that includes the four elements highlighted in NSPM-33:

(1) Cybersecurity (see Subsection 6 below)

(2) Foreign travel security. Agencies should require that research organizations maintain international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, research purposes, or any offers of sponsored travel that would put a person at risk. Such policies should include an organizational record of covered international travel by faculty and staff and, as appropriate, a disclosure and authorization requirement in advance of international travel, security briefings, assistance with electronic device security (smartphones, laptops, etc.), and pre-registration requirements.

(3) Research security training. Agencies should require that, as part of their research security programs, research organizations provide training to relevant personnel on research security threat awareness and identification, including insider threat training where applicable. Research organizations should consider incorporating relevant elements of research security into existing training on responsible and ethical conduct of research for faculty and students. In addition to periodic training, research organizations should conduct tailored training in the event of a research security incident.

(4) Export control training, as appropriate. Agencies should require that research organizations conducting R&D that is subject to export control restrictions provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists.

Agencies should require that, as part of their research security program, research organizations designate a research security point of contact (POC) and provide publicly accessible means to contact that individual (such as through a website or social media).

Organizations conducting research involving classified or controlled unclassified information (CUI) may combine research security POCs, but such research will otherwise remain subject to already-established security protocols in addition to the more broadly applicable standards associated with the NSPM-33 research security program requirement. Agencies should not require that research organizations apply the more stringent security protocols appropriate to classified information or CUI to the conduct of fundamental research.

2. *Determination of which research organizations are subject to the requirement*

Qualifying research organizations should be those that met the $50 million threshold in total Federal science and engineering support for the previous two fiscal years, as recorded on USASpending.gov.

3. *Standardization of program requirements across organizations*

All qualifying research organizations, as defined above, should be subject to the standard requirements described in subsection 1 of this section. For any instances in which research agencies determine that additional research security program elements are necessary for Federal R&D funding in critical and emerging technology areas with implications for U.S. national and economic security, the associated requirements should be included within R&D award terms and conditions.

4. *Process for finalizing and implementing the requirement*

OSTP, in consultation with the NSTC Subcommittee on Research Security, OMB, and external stakeholders, will develop a standardized requirement for uniform implementation across research agencies. Following a 90-day external engagement period, OSTP will complete the standardized requirement in the subsequent 120 days, and, upon completion, work with OMB to develop a plan to implement the standardized requirement. Upon receipt of the standards, relevant research agencies should engage with external stakeholders to ensure that program requirements are appropriate to the broad range of organizations that are subject to the requirement.

5. *Development of research security program content*

The Federal Government will provide standardized technical assistance to support development of training content and programmatic guidelines, tools, and best practices to be made available to organizations for incorporation into research security programs at their discretion. In particular, agencies represented on the National Counterintelligence Task Force, in conjunction with the National Counterintelligence and Security Center, will jointly develop content that research organizations can leverage to meet requirements for research security programs and training. In concert, the Federal Government should consider supporting the formation of a community consortium to develop and maintain research security program information and implementation resources for research organizations, to include resources suitable for use within research security programs. To the greatest extent practicable, development of program content should be a collaborative effort between the government and organizations.

6. *Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement*

Agencies should require that research organizations satisfy the cybersecurity element of the research security program requirement by applying the following basic safeguarding protocols and procedures:

- Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches.
- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- Verify and control/limit connections to and use of external information systems.
- Control any non-public information posted or processed on publicly accessible information systems.
- Identify information system users, processes acting on behalf of users, or devices.
- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
- Identify, report, and correct information and information system flaws in a timely manner.
- Provide protection from malicious code at appropriate locations within organizational information systems.
- Update malicious code protection mechanisms when new releases are available.
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Additional cybersecurity requirements, for example, those provided by the National Institute of Standards and Technology (NIST), will apply in some cases, such as for research involving classified information or CUI.

7. *Certification of compliance with the requirement*

Once the research security requirement is finalized and further guidance is available, it is expected that research organizations will be required to provide certification of compliance with the research security program requirement. OSTP, in consultation with the NSTC Subcommittee on Research Security and OMB plan to develop a single certification standard and process that will apply across all research agencies. This approach will be less burdensome than integrating an organizational certification into the R&D award application process.

Research organizations are required to maintain a description of the research security program, and to provide such documentation within 30 days of a request from a research agency that is funding an R&D award or considering an application for R&D award funding to that research organization. In addition, research agencies should consider integrating the research security program requirement into the Compliance Supplement's Research and Development Cluster audit guidance as part of the single audit of Federal grant and assistance programs (2 C.F.R. Part 200, Appendix XI).

8. *Discretion of research organizations in structuring research security programs*

Research organizations should be provided flexibility to structure the organization's research security program to best serve its particular needs, and to leverage existing programs and activities where relevant, provided that the organization implements all required program components. Some research organizations may choose to integrate research security requirements into existing programs—such as existing cybersecurity programs and responsible and ethical conduct in research training—to maximize efficiency. Research organizations should be strongly encouraged to integrate some or all elements into a coherent research security program, where applicable and feasible.

9. *Timeline for research organizations to establish compliance*

Qualifying research organizations should establish a research security program as soon as possible, but should be provided one year from date of issuance of the formal requirement to comply. Organizations that become subject to the requirement in subsequent years should similarly be provided one additional year to comply.

Appendix: Definitions

Conflict of commitment – Situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time and effort, including obligations to dedicate time in excess of organizational or research agency policies or commitments. Other types of conflicting obligations, including obligations to improperly share information with, or to withhold information from, an employer or research agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment used in this document.

Conflict of interest – Situation in which an individual, or the individual's spouse or dependent children, has a significant financial interest, or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.

Controlled unclassified information (CUI) – Information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and Government-wide policies, but is not classified.

Covered individual or **Senior/key personnel** – an individual who (a) contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a Federal research agency; and (b) is designated as a covered individual by the Federal research agency concerned. Consistent with NSPM-33, this means principal investigators (PIs) and other senior/key personnel seeking or receiving Federal research and development funding (i.e., extramural funding) and researchers at Federal agency laboratories and facilities (i.e., intramural researchers, whether or not federally employed), including Government-owned, contractor-operated laboratories and facilities.

Current and pending research support – (a) All resources made available, or expected to be made available, to an individual in support of the individual's research and development efforts, regardless of (i) whether the source is foreign or domestic; (ii) whether the resource is made available through the entity applying for a research and development award or directly to the individual; or (iii) whether the resource has monetary value; and (b) includes in-kind contributions requiring a commitment of time and directly supporting the individual's research and development efforts, such as the provision of office or laboratory space, equipment, supplies, employees, or students. This term has the same meaning as the term **Other Support** as applied to researchers in NSPM-33: For researchers, Other Support includes *all* resources made available to a researcher in support of and/or related to *all* of their professional R&D efforts, including resources provided directly to the individual rather than through the research organization, and regardless of whether or not they have monetary value (e.g., even if the support received is only in-kind, such as office/laboratory space, equipment, supplies, or employees). This includes resource and/or financial support from all foreign and domestic entities, including but not limited to, gifts provided with terms or conditions, financial support for laboratory personnel, and participation of student and visiting researchers supported by other sources of funding.

Digital persistent identifier (DPI or digital PID) – A digital identifier that is globally unique, persistent, machine resolvable and processable, and has an associated metadata schema. Consistent with NSPM-33, digital persistent identifiers for individuals are used to disambiguate and identify an individual person.

Research Organization – An entity that has applied for or received an R&D award from a Federal research agency. This term has the same meaning as "entity" as defined in Section 223 of the NDAA for 2021.

Federal research agency or Research agency – Any Federal department or agency with an annual extramural research expenditure of over $100,000,000. This term has the same meaning as "funding agency" in NSPM-33.

Foreign government-sponsored talent recruitment program – Effort organized, managed, or funded by a foreign government, or a foreign government instrumentality or entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position). Some foreign government-sponsored talent recruitment programs operate with the intent to import or otherwise acquire from abroad, sometimes through illicit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government. Many, but not all, programs aim to incentivize the targeted individual to relocate physically to the foreign state for the above purpose. Some programs allow for or encourage continued employment at United States research facilities or receipt of Federal research funds while concurrently working at and/or receiving compensation from a foreign institution, and some direct participants not to disclose their participation to United States entities. Compensation could take many forms including cash, research funding, complimentary foreign travel, honorific titles, career advancement opportunities, promised future compensation, or other types of remuneration or consideration, including in-kind compensation.

Gift – Includes any gratuity, favor, discount, entertainment, hospitality, loan, forbearance, license, special access, equipment time, samples, research data, or other item having monetary value. A gift also includes services as well gifts of training, transportation, local travel, lodging, meals, research hours, whether provided in-kind, by purchase of a ticket, payment in advance, or reimbursement after the expense has occurred. A gift by definition is given without expectation of anything in return.

Honorarium – A payment of money or anything of value for an appearance, speech, article, or other form of compensation or award.

Insider threat – The potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.[11]

Intramural Researcher – An agency employee who conducts research supported by the agency in which they are employed.

Research and development (R&D) – Incudes basic research, applied research, and experimental development. Basic research is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts. Applied research is original investigation undertaken in order to acquire new knowledge, and directed primarily towards a specific practical aim or objective. Experimental development is creative and systematic work, drawing on knowledge gained from research and practical experience, which is

[11]https://www.cisa.gov/sites/default/files/publications/Insider%20Threats%20101%20What%20You%20Need%20to%20Know_508.pdf

directed at producing new products or processes or improving existing products or processes. Like research, experimental development will result in gaining additional knowledge. Experimental development includes the production of materials, devices, and systems or methods, including the design, construction, and testing of experimental prototypes. Experimental development also includes technology demonstrations in cases where a system or component is being demonstrated at scale for the first time, and it is realistic to expect additional refinements to the design (feedback R&D) following the demonstration.[12]

Research and development award – Support provided to an individual or entity by a Federal research agency to carry out R&D activities, which may include support in the form of a grant, contract, cooperative agreement, or other such transaction. The term does not include a grant, award, contract, agreement, or other transaction for the procurement of goods or services to meet the administrative needs of a Federal research agency.

Research integrity – The use of honest and verifiable methods in proposing, performing, and evaluating research; reporting research results with particular attention to adherence to rules, regulations, and guidelines; and following commonly accepted professional codes or norms.

Research security – Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

United States Government supported research and development – Includes R&D projects funded by the U.S. Government, in whole or in part; projects that use U.S. Government equipment or facilities for conducting R&D; and R&D projects in which U.S. Government employee and contractor personnel participate, regardless of the project's funding source.

[12] https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf