NSPM 33 Policy Memorandum

NSPM 33 Policy Memorandum

Table of Contents

Introduction

On January 14, 2021, President Donald Trump issued a National Security Policy memorandum aimed at strengthening protections for U.S. government-sponsored Research and Development (R&D) against foreign interference and exploitation. This directive underscored the critical role that R&D plays in driving scientific and technological innovation, bolstering the U.S. economy, and ensuring national security. At the heart of the policy was a growing concern that certain foreign governments, particularly the People's Republic of China, were leveraging the openness of the U.S. research enterprise to their strategic advantage—reaping the benefits of American scientific progress without reciprocating transparency or investment.

The memorandum outlined a series of robust measures to safeguard U.S. intellectual capital while maintaining an environment that fosters innovation and international collaboration.
It called for stricter disclosure requirements, enhanced security protocols, and reinforced consequences for violations of research integrity. It also emphasized the need for coordination across federal agencies, academia, and private industry to mitigate risks associated with foreign government-sponsored talent recruitment programs and unauthorized access to sensitive research.

This policy represented a pivotal moment in the U.S. government's approach to research security, balancing the nation's commitment to open scientific exchange with the imperative to protect its technological and economic interests. By examining the key provisions of this memorandum, we can better understand the challenges facing the U.S. R&D enterprise and the steps being taken to ensure its continued leadership on the global stage.

Purpose

The purpose of this memorandum is to strengthen the protection of U.S. government-endorsed Research and Development (R&D) against foreign government interference and exploitation. This R&D is a crucial driver of Science and Technology (S&T) innovation and is vital to the U.S. economy and national security.

A significant portion of U.S. government-funded R&D is widely distributed and encompasses both fundamental research, as defined by National Security Decision Directive (NSDD)-189, and scientific studies utilizing publicly available data. The open and collaborative nature of the U.S. R&D enterprise strengthens America's innovation, leadership in science and technology, economic competitiveness, and national security.

However, certain foreign governments, including the People's Republic of China, have not demonstrated a reciprocal commitment to open scientific exchange and instead seek to take advantage of U.S. and international research environments. This approach allows China to bypass the costs and risks associated with conducting research, bolstering its economic and military ambitions while undermining the U.S., its allies, and global partners.

While sustaining an open environment to foster research discoveries and innovation that benefit our nation and the world, the U.S. will also take steps to safeguard intellectual capital, prevent research theft, and ensure responsible management of U.S. taxpayer dollars. This includes measures to ensure that participants with significant influence on the U.S. R&D enterprise fully disclose information that could reveal potential conflicts of interest and conflicts of commitment.

Definitions

President Trump assigned these agencies the responsibility of understanding key definitions within this memorandum. Each term serves a specific purpose in this directive.

1. Participants in the United States R&D Enterprise – This term refers to researchers at academic and independent research institutions, medical centers, private establishments, and federal government research centers and laboratories. It also includes individuals involved in allocating and awarding federal R&D funding.

2. United States Government-Supported R&D – This refers to fully or partially funded U.S. government R&D projects. It includes projects utilizing U.S. government equipment or facilities for conducting R&D, as well as projects involving U.S. government employees and contractor personnel, regardless of the project's funding source.

3. Conflict of Interest (COI) – This refers to situations in which an individual, their spouse, or dependent children have a financial interest or relationship that could directly and significantly affect the design, conduct, reporting, or financing of research.

4. Conflict of Commitment (COC) – This refers to situations where an individual incurs conflicting obligations between multiple employers or entities. Many agencies define conflicts of commitment as situations where time and effort become conflicted, including obligations that exceed institutional or agency policies.

5. Foreign Government-Sponsored Talent Recruitment Program – These programs are efforts, directly or indirectly organized, managed, or subsidized by a foreign government or institution to recruit S&T professionals or students, regardless of citizenship or national origin. Some of these programs aim to acquire technology, software, or intellectual property, and may provide compensation to participants.

6. Federal Personnel – This term refers to officers and employees of the U.S. government and members of the uniformed services, including those in the Reserve Components.

7. Digital Persistent Identifier (DPI) – A unique digital identifier that permanently and unmistakably identifies a digital object or an individual.

Roles and Responsibilties

Each agency has specific roles and responsibilities to fulfill in their respective domains. Executive departments and agency heads that fund R&D activities must complete the following tasks in accordance with applicable law:

1. Require that participants in the U.S. R&D enterprise who significantly influence the design, conduct, reporting, reviewing, or funding of federally funded research disclose relevant information to enable consistent determinations of conflicts of interest and commitment.

2. Ensure that organizations receiving federal funds have established policies and processes to identify and manage risks to research security and integrity.

3. Collaborate with agency Inspectors General and law enforcement agencies to identify disclosures that may negatively impact research funding, security, or integrity.

4. Coordinate with agency Inspectors General and law enforcement to investigate suspected failures to comply with disclosure requirements.

5. Ensure appropriate and effective consequences for violations of disclosure policies and engagement in activities that threaten the security and integrity of the U.S. R&D enterprise.

The Secretary of Homeland Security will ensure that the Department of Homeland Security (DHS), in collaboration with the Department of State, screens foreign nonimmigrant students or exchange visitors contributing to the U.S. R&D sector for potential national security threats.

The Director of National Intelligence (DNI) will oversee intelligence efforts to evaluate foreign entities' activities related to U.S. research security.

The Director of the Office of Science and Technology Policy (OSTP) will lead efforts to protect federally funded R&D from foreign government interference and engage with the U.S. scientific and academic communities to raise awareness of research security risks.

Priorities

Federal agencies must align their efforts to meet key priorities, each with distinct objectives.

Enhancing Awareness of Research Security Risks and Protections

1. In coordination with applicable law, the OSTP Director, DNI, and other agency leaders will work with the U.S. R&D enterprise to increase awareness of risks to research security and integrity. These efforts will:

2. Explain threats posed by some foreign government-sponsored efforts, including talent recruitment programs.

3. Describe federal policies and actions to mitigate risks.

4. Outline procedures for research institutions to enhance security.

5. Increase awareness of existing laws, regulations, and mechanisms to prevent unauthorized transfers of U.S. technology and intellectual property.

6. The DNI will develop intelligence products to support federal, state, local, and tribal officials, research institutions, private sector entities, and U.S. allies in identifying and mitigating research security threats.

The DNI will develop intelligence products to support federal, state, local, and tribal officials, research institutions, private sector entities, and U.S. allies in identifying and mitigating research security threats.

The DNI, in coordination with the heads of other agencies, shall refine data and intelligence products associated with research security for dissemination, in accordance with applicable law, to other agencies.

The information shall be sent to federal, state, local, and tribal officials, research institutions, the private sector, and allies and partners. These materials aim to:

- Explain foreign government-supported collection methods and means of exploitation.

- Help identify R&D activities and collaborations with significant risk of exploitation.

- Provide counterintelligence awareness training.

Strengthen Disclosure Requirements and Processes

The leaders of U.S. research funding agencies will mandate that other agencies disclose information regarding potential conflicts of interest and commitment among participants in federally funded R&D activities. This information should be shared with organizations applying for or receiving federal funding, the funding agency, or both, in accordance with agency policies and relevant laws and regulations. While disclosure requirements may differ based on an individual's role within an organization, they should not replace existing disclosure obligations established by law and the U.S. Office of Government Ethics regulations, which apply to certain entities within the U.S. R&D enterprise.

Agencies must require disclosure, where consistent with relevant U.S. law, regulation, contract, agreement, and award, from the following divisions of the federally funded R&D enterprise:

- Principal investigators (PIs) and other senior/key personnel seeking or receiving federal R&D funding (i.e., extramural funding).

- Individuals participating in the process of allocating federal funding, including program officers, peer/merit reviewers, and members of advisory panels and committees.

- Researchers at federal agency laboratories and facilities, including government-owned, contractor-operated laboratories and facilities.

Agencies will require the following disclosures, where consistent with relevant U.S. law, regulation, contract, agreement, and award, depending on the individual's role in the U.S. R&D enterprise:

- Organizational affiliations and employment.
- Other support, contractual or otherwise, direct and indirect, including current and pending private and public sources of funding or income, both foreign and domestic.
- Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs.
- Positions and appointments, both domestic and foreign, including affiliations with foreign entities or governments.

When agencies find that someone has violated the terms of an agreement, they may consider a range of consequences, including but not limited to the following:

- Termination of federal employment or contract.
- Termination of a grant, cooperative agreement, contract, or award.
- Preserving a grant, cooperative agreement, contract, or award, but requiring or otherwise ensuring that individual(s) do not perform work under the grant, contract, or award.
- Ineligibility for participation in U.S. government review panels and other activities.
- Suspension or debarment of eligibility for federal funding.
- Suspension or denial of Title IV funds.

Limit Access and Participation

Agency leaders must ensure that their respective agencies have policies and processes to control and track access to and utilization of U.S. government research facilities, consistent with applicable law and appropriations. These should include provisions for directing and tracking physical access, vetting and securely hosting foreign visitors, and evaluating research partnerships or contracts with outside entities.

Vetting Foreign Students and Researchers

The Secretary of State, in coordination with the Secretary of Homeland Security, shall ensure that vetting processes for foreign students and researchers reflect the evolving risks to U.S. R&D. The Secretary shall take necessary steps to ensure consular officers can collect and consider the following information regarding visa applicants, based on relevant U.S. legal standards:

- Employment and employment history.
- Sources of financial support.
- Education history, including academic institutions, degrees, and research advisors.
- Current and prior R&D affiliations and projects.
- Current and pending participation in foreign government-sponsored talent recruitment programs.
- Program of study and/or research.
- Facility or facilities and location(s) of expected work.

Information Sharing

To strengthen the effectiveness of response measures, heads of agencies must share information about violators across federal funding institutions and with federal law enforcement agencies, DHS, and state authorities. Such sharing must align with privacy laws and other legal restrictions and must not interfere with law enforcement or intelligence activities. Agency heads should consider the privacy of organizational data and ensure it is protected.

Training Programs

The leaders of funding agencies must ensure that federal personnel involved in R&D activities or in the allocation of federal R&D funding receive research security training. This training should cover, as appropriate, risks to the U.S. R&D enterprise, individuals' responsibilities regarding research security and integrity, and behaviors or situations that may indicate potential security risks. Training programs should include an initial orientation for new employees and annual refresher courses.

Risk Identification and Analysis

Within 12 months of this memorandum's issuance, the heads of funding agencies must require research institutions receiving over $50 million annually in federal science and engineering support to certify to the funding agency that they have established and maintain a research security program. These programs should incorporate elements such as cybersecurity, foreign travel security, insider threat awareness and detection, and, where applicable, export control training. Additionally, funding agency heads will evaluate whether further research security requirements are necessary for institutions receiving federal R&D funding in critical and emerging technology fields that impact U.S. national and economic security.

Promoting and Protecting International R&D Cooperation

The Secretary of State, in conjunction with the Director of OSTP and the heads of other agencies, shall engage with foreign allies and partners to promote policies and practices that increase awareness of risks to research security and improve cooperation on international protection and response efforts. Messaging should be designed to increase awareness and encourage foreign governments to implement effective practices to assess and mitigate risks to research security and integrity.

Implementation

The APNSA, in coordination with the Director of OMB and the Director of OSTP, must oversee the implementation of this memorandum.

On an annual basis, all three will prepare and submit a report to the President detailing activities taken by funding agencies to implement this memorandum.

General Provisions

Nothing in this memorandum shall be interpreted as limiting or otherwise affecting the legal authority of any executive department, agency, or its leadership, nor the responsibilities of the Director of the Office of Management and Budget regarding budgetary, administrative, or legislative matters.

The implementation of this memorandum shall be consistent with applicable laws and presidential directives and is subject to the availability of appropriations.

This memorandum does not create any rights or benefits, whether substantive or procedural, that are enforceable by any party against the United States, its departments, agencies, entities, officers, employees, agents, or any other individual.

Conclusion

The National Security Policy Memorandum on Cybersecurity, issued by President Donald Trump on January 14, 2021, underscores the urgent need to safeguard U.S. government-supported research and development (R&D) from foreign interference and exploitation. By defining key terms, clarifying agency roles, setting clear priorities, and outlining implementation strategies, the memorandum establishes a comprehensive framework for protecting America's scientific and technological advancements.

The memorandum highlights the importance of research security while maintaining an open and collaborative environment that fosters innovation. Recognizing the growing threats from foreign adversaries—particularly nations like China—it seeks to ensure transparency, enforce disclosure requirements, and impose consequences for noncompliance. Additionally, by prioritizing risk identification, international cooperation, and training programs, the policy aims to enhance national security without stifling scientific progress.

In a rapidly evolving global landscape, where technological supremacy is increasingly linked to national security, this policy memorandum plays a fundamental role in strengthening the integrity of U.S. research institutions.

By implementing its provisions, the United States reaffirms its commitment to protecting intellectual property, securing taxpayer-funded research, and maintaining its competitive edge in science and technology. While challenges remain, this memorandum lays the groundwork for a more resilient and secure research ecosystem—one that continues to drive innovation while safeguarding the nation's economic and security interests.

Endnotes

1. Presidential Memorandum on United States Government-Supported Research and Development National Security Policy, 2021 Daily Comp. Pres. Doc. 37 (Jan. 14, 2021), https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

For more information, contact:

Authors

Lee Zeichner
CEO
lee@zra.com
(703) 868-8769

Zeichner Risk Analytics

4601 Fairfax Dr #1130, Arlington, VA 22203
(703) 351-1101

5661 Beaumont Avenue, San Diego, CA 92037
(703) 868-8769