COMMITTEE ON
SCIENCE, SPACE AND TECHNOLOGY
CHAIRMAN FRANK LUCAS

FULL COMMITTEE

HEARING CHARTER

"Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise"

Thursday, February 15, 2024
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

The purpose of this hearing is to examine the actions taken by federal science agencies to implement recent guidance and laws to protect proprietary technology and scientific discoveries, including the *Guidance for Implementing NSPM-33 on National Security Strategy for United States Government-Supported Research and Development* and the research security provisions in the 2020 and 2021 National Defense Authorization Acts and the Chips and Science Act of 2022. The Committee will discuss the status of implementation of these provisions across the federal government, barriers to compliance, as well as newly identified risks and threats to the security of federally funded research. The hearing will also examine the implications of undue foreign influence for researchers, research institutions, and the competitiveness of the U.S. research enterprise.

Witnesses

- **The Honorable Arati Prabhakar,** Director, White House Office of Science and Technology Policy
- **Dr. Rebecca Keiser,** Chief of Research Security Strategy and Policy, National Science Foundation
- **The Honorable Geri Richmond,** Under Secretary for Science and Innovation, Department of Energy
- **Dr. Michael Lauer,** Deputy Director for Extramural Research, National Institutes of Health

Overarching Questions

- What is the status of research security activities at federal science agencies? What is the timeline for full compliance with existing statutes and executive branch guidance?
- How are federal science agencies coordinating to ensure uniformity in the implementation of research security guidance and requirements?
- How are federal science agencies and the broader research community engaging with law enforcement and the intelligence community to understand and address the threat of malicious actors exploiting our open system of science?
- What actions are being taken to engage with the broad research community to communicate appropriate training requirements and best practices for identifying research security risks?
- Why is it important for the U.S. to balance security risks and the importance of scientific openness and international collaboration? How will our implementation of research security requirements impact U.S. competitiveness?

BACKGROUND

Openness is one of the most important tenets of scientific research. Broad dissemination of results and data and the free exchange of ideas facilitate wider evaluation and confirmation of results and spark new collaborations and avenues of inquiry. Openness increases the validity of research results, improves productivity and student training, and helps deliver the benefits of research to the broader public. It also enables the scientific community to identify and correct for instances of scientific misconduct, such as fabrication or falsification of data, enhancing the integrity of the entire research enterprise and building accountability and public trust.

While there are domains in which openness in science can be detrimental to national competitiveness or security, fundamental research has been generally exempted from security restrictions since 1985. President Reagan's National Security Decision Directive 189 (NSDD-189) defines fundamental research as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." It also dictates that "to the maximum extent possible, the products of fundamental research remain unrestricted," and specifies that "where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification."[1]

The directive does not claim that the open sharing of fundamental research is without risk. Rather, it asserts that openness in research is so important to competitiveness and security that it warrants the risk that adversaries may benefit from scientific openness as well.

[1] The White House. (1985, September 21). NSDD 189 National Policy on Transfer of Scientific, Technical and Engineering Information. National Archives Catalog. https://catalog.archives.gov/id/6879779.

In recent years, several incidents have led to the concern that other countries are taking advantage of the openness of the academic research environment in the United States, underscoring the need to balance a commitment to openness with the potential threats posed by foreign actors seeking to exploit, degrade and misappropriate America's open system of science.[2] Threats to research security primarily arise from the failure of researchers applying for federal funding to disclose foreign affiliations, such as participation in a foreign talent recruitment program, conflicts of commitments, and sources of funding that may present a conflict of interest (COI). Because federal science agencies award research grants to institutions, not the individual researcher, institutions are primarily responsible for ensuring compliance with these policies.

Funding agencies are usually alerted to allegations of noncompliance, through notification from the awardee's institution, an anonymous tip, or another audit or investigation. At that point they coordinate with the institution to assess the available evidence and determine if an agency action is necessary. In many cases, an agency works with the university and researcher to bring them into compliance and ensure expectations are clearly communicated. If the agency suspects a researcher engaged in intentional deception, misconduct, or fraud, the agency can refer the case to the Office of the Inspector General (OIG) for further investigation. In addition, the OIG can and does initiate its own investigations, and when appropriate, refers criminal cases to the Department of Justice (DOJ).

Research integrity is a set of ethical standards that form the foundation for responsible conduct of research: objectivity, honesty, openness, accountability, fairness, and stewardship.[3] Research security can be defined as "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."[4] For example, malign foreign talent recruitment programs have been found to incentivize or coerce participants to acquire "through illicit as well as licit 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."[5] Funding agencies and DOJ have identified and cracked down on several specific behaviors, including:

- failure to disclose conflicts of financial and non-financial interest, including funding, parallel laboratories, employment, affiliations, and appointments;

---

[2] JASON, The MITRE Corporation. *Fundamental Research Security*. December 2019. McLean, VA. Available at https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[3] National Academies of Sciences, Engineering, and Medicine. 2017. Fostering Integrity in Research. Washington, DC: The National Academies Press. https://doi.org/10.17226/21896.

[4] National Science and Technology Council, Subcommittee on Research Security and Joint Committee on the Research Environment, "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development," January 2022, available at https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

[5] National Science & Technology Council, Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise. January 2021. Available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf.

- failure by peer reviewers to keep information in grant applications confidential, including disclosure to foreign entities or other attempts to influence funding decisions; and
- diversion of intellectual property in grant applications or produced by agency-supported research to other entities, including other countries.

Participation in a foreign talent recruitment program is not necessarily improper. However, in recent years, research funding agencies have uncovered a correlation between noncompliance with COI and disclosure requirements and participation in Chinese-government sponsored malign talent recruitment programs.[6]

EXECUTIVE BRANCH ACTIONS

White House Office of Science and Technology Policy and Interagency Workgroups

In the last few years, multiple government entities have written or commissioned guidance documents in an attempt to define known threats to the U.S. research enterprise.

In February 2019, then-Director of the White House Office of Science and Technology Policy (OSTP), Kelvin Droegemeier, announced that "ensuring the safety and security of researchers and our innovations" was among OSTP's top policy priorities.[7] As OSTP Director, Droegemeier also served as chair of the National Science and Technology Council (NSTC) – a cabinet-level advisory body composed of representatives from federal science agencies that was created by executive order to coordinate science and technology (S&T) policy.[8] Historically, OSTP and the NSTC have worked together to coordinate the development and implementation of research and development (R&D) policies across federal science agencies. In keeping with this precedent, the NSTC convened a new body of agency representatives to prioritize the coordination of research security policies.

In May 2019, the NSTC formed the Joint Committee on Research Environments (JCORE) "to address the most pressing challenges facing America's research and scientific community."[9] JCORE established four subcommittees to coordinate its work: the Subcommittee on Safe and Inclusive Research Environments, the Subcommittee on Rigor and Integrity in Research, the Subcommittee on Reducing Administrative Burdens, and the Subcommittee on Research Security.[10]

---

[6] *Id.*
[7] Droegemeier quoted in William Thomas, "Droegemeier Outlines Agenda in First Speech as OSTP Director," FYI: Science Policy News, February 20, 2019, https://ww2.aip.org/fyi/2019/droegemeier-outlines-agenda-first-speech-ostp-director.
[8] CRS Report R47635, *The White House Office of Science and Technology Policy: Issues and Options for the 118th Congress*, by Emily G. Blevins and Rachael F. Roan.
[9] The White House Office of Science and Technology Policy, Update from the National Science and Technology Council Joint Committee on Research Environments, July 9, 2019, https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/07/Update-from-the-NSTC-Joint-Committee-on-Research-Environments-July-2019.pdf;
[10] *Id.*

In December 2019, just over six months after its launch, Congress codified the ongoing work of the NSTC's JCORE Subcommittee on Research Security in the "Securing American Science and Technology Act" as part of the National Defense Authorization Act (NDAA) for Fiscal Year 2020.[11] The bill also directed the National Science Foundation (NSF), the Department of Energy (DOE), the Department of Defense (DOD), and other agencies to enter into a joint agreement with the National Academies of Science, Engineering, and Medicine to establish a National Science, Technology, and Security Roundtable to identify best practices for communicating threats and risks to federally funded R&D, among other purposes.[12]

On January 14, 2021, President Trump issued National Security Presidential Memorandum 33 (NSPM-33), "*Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*," which tasked OSTP and the Subcommittee on Research Security with coordinating the implementation of these provisions across federal agencies to secure federally funded R&D.[13] NSPM-33 directs actions by funding agencies to secure intellectual capital while acknowledging the importance of openness and scientific collaboration. These include:

- prohibiting Federal personnel from participating in foreign-government-sponsored talent recruitment programs;
- requiring institutions of higher education to develop research security programs;
- directing agencies and universities to share information about individuals whose behavior poses a risk to research integrity and security;
- directing the Department of State and the Department of Homeland Security to review vetting processes for foreign students and researchers;
- directing agencies to harmonize disclosure processes and definitions; and
- streamlining the grant application process through the use of digital persistent identifiers (DPI).

In response, OSTP and the Subcommittee on Research Security have issued several publications containing guidance for federal agencies to implement the research security requirements outlined in NSPM-33, including the following:

- NSTC JCORE Subcommittee on Research Security, *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*, January 2021;[14]
- White House, OSTP, NSPM-33 Fact Sheet, "President Trump Takes Bold Action to Strengthen the Security and Integrity of America's Research and Development Enterprise," January 2021;[15]

---

[11] P.L. 116-92, Div. A, Title XVII, §1746(a).
[12] P.L. 116-92, Div. A, Title XVII, §1746(b).
[13] The White House, "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," January 14, 2021, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.
[14] *supra* note 5
[15] The White House, *President Trump Takes Bold Action to Strengthen the Security and Integrity of America's*

- White House, OSTP Blog Post by Eric Lander, "Clear Rules for Research Security and Researcher Responsibility," August 10, 2021;[16]
- White House, OSTP Blog Post by Eric Lander, "Guidance for U.S. Scientific Research Security That Preserves International Collaboration," January 4, 2022;[17]
- NSTC JCORE Subcommittee on Research Security, Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States-Government-Supported Research and Development, January 2022;[18]
- Memorandum from Alondra R. Nelson, Deputy Director for Science and Society, OSTP, to Heads of Member Agencies of the National Science and Technology Council, "Re: Next Steps on NSPM-33 Implementation," March 1, 2022;[19] and
- White House, OSTP, Updates on Research Security Policies and Practices in the U.S. Government, October 2022.[20]

In February 2023, the NSTC Subcommittee on Research Security released a "Draft Research Security Programs Standard Requirement" to facilitate implementation of Section 4(g) of NSPM-33.[21] The draft guidance provided additional details on covered organizations, foreign travel security, research security training, cybersecurity, and export control training. It also specified that federal agencies should communicate the required training components and standards to research organizations as part of their funding agreement processes. A revised version of the draft guidance was posted in the Federal Register for public comment on March 7, 2023.[22]

National Science Foundation

In December 2019, JASON issued an NSF-commissioned report titled "Fundamental Research Security".[23] JASON is an independent science advisory group that contracts with government

---

Research and Development Enterprise. January 2021. Fact Sheet. Available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSC-OSTP-NSPM33-Fact-Sheet-Jan2021.pdf.

[16] Lander , E. (2021, August 10). Clear rules for research security and researcher responsibility. The White House. https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/

[17] Lander , E. (2022, January 4). Guidance for U.S. Scientific Research Security that preserves international collaboration. The White House. https://www.whitehouse.gov/ostp/news-updates/2022/01/04/guidance-for-u-s-scientific-research-security-that-preserves-international-collaboration/

[18] *supra* note 4.

[19]Office of Science and Technology Policy , & Nelson, A., White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/03/03-2022-Coordination_RS_Letter.pdf.

[20] Executive Office of the President of the United States, Updates on Research Security Policies and Practices in the U.S. Government. Office of Science and Technology Policy . Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/10/WHOSTP_ResearchSecurity_CommunityBriefingSlides.pdf.

[21] NSTC Subcommittee on Research Security, "Draft Research Security Programs Standard Requirement," February 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

[22] OSTP, Request for Information; NSPM 33 Research Security Programs Standard Requirement, 88 Federal Register 14187, April 7, 2023, https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement.

[23] Long, G., National Science Foundation (2019). The MITRE Corporation. Retrieved February 7, 2024, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

agencies to produce reports on matters of defense science and technology.[24] The report affirmed the importance of foreign scientific talent, warned against placing new restrictions on access to fundamental research, and acknowledged the difficulty in assessing the scale and scope of legitimate threats to research security. It concluded by stating that "many of the problems of foreign influence that have been identified are ones that can be addressed within the framework of research integrity."

Prior to the JASON report, NSF issued a policy prohibiting NSF employees and rotators from participating in foreign talent recruitment programs in July 2019.[25] Then in February 2020, NSF clarified that its disclosure requirement for grant applicants includes both foreign and domestic sources of support.[26] In March 2020, NSF established a new Chief of Research Security Strategy and Policy position.[27]

In September 2021, in partnership with the National Institutes of Health (NIH), NSF implemented a new digital format for submitting researcher biographical sketches as part of grant applications to simplify and standardize the disclosure process for researchers seeking funding from both agencies.[28] Then, acting on behalf of the Subcommittee on Research Security, in August 2022, NSF released two draft common disclosure forms for public comment to enhance disclosure requirements and reduce the administrative burden on grant applicants.[29] NSF released the final versions[30] of the common disclosure forms along with an updated list of relevant definitions in November 2023.[31]

NSF has also updated its draft version of the Proposal and Award Policies and Procedures Guide to include requirements for institutions of higher education to disclose current financial support of $50,000 or more from a foreign source, directly or indirectly.[32] Most recently, NSF launched

---

[24] Aftergood, St. (Ed.). (n.d.). Jason Defense Advisory Panel reports. JASON Defense Advisory Panel: Reports on Defense Science and Technology. https://irp.fas.org/agency/dod/jason/.

[25]Office of the Director , Personnel Policy on Foreign Government Talent Recruitment Programs (2019). National Science Foundation. Retrieved from https://www.nsf.gov/bfa/dias/policy/researchprotection/PersonnelPolicyForeignGovTalentRecruitment%20Programs07_11_2019.pdf.

[26] NSF Grants. (2020b, February 18). 2/6/20 PAPPG webinar - training for the External Community. YouTube. https://www.youtube.com/watch?v=OgZHhoHTqf4.

[27] NSF News - NSF creates new research security chief position. NSF. (2020, March 2). https://new.nsf.gov/news/nsf-creates-new-research-security-chief-position

[28] Documents required for senior personnel. NSF. (n.d.). https://new.nsf.gov/funding/senior-personnel-documents#biographical-sketch-0bd.

[29] National Science Foundation on behalf of the National Science and Technology Council's Research Security Subcommittee, "Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support," 87 *Federal Register* 53505-53507, August 31, 2022.

[30] NSF, "NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization," https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp.

[31] NSF, National Security Presidential Memorandum-33 Implementation Guidance Appendix: Definitions, November 1, 2023, https://www.nsf.gov/bfa/dias/policy/researchprotection/nspm33definitions.pdf.

[32] National Science Foundation, "Agency Information Collection Activities: Comment Request; National Science Foundation Proposal/Award Information-NSF Proposal and Award Policies and Procedures Guide," 88 Federal Register 22488, April 13, 2023, https://www.federalregister.gov/documents/2023/04/13/2023-07780/agency-information-collection-activities-comment-request-national-science-foundation-proposalaward.

four interactive online research security training modules for U.S. researchers and institutions to provide clear guidelines and effective strategies to protect against existing and emerging threats.[33]

National Institutes of Health

NIH established a Working Group on Foreign Influence on Research Integrity, which released a report in December 2018 with recommendations for NIH and universities on raising awareness of foreign influence and safeguarding research integrity.[34] NIH then issued a reminder to the research community of their full disclosure requirements in March 2018.[35] In 2020, NIH issued policies and provided internal training to protect confidentiality in the peer review process.[36, 37] In December 2022, NIH partnered with NSF to fund the four research security training module awards focused on the importance of research security, the importance of disclosure, risk management and mitigation, and international collaboration (also referred to in the NSF section.)[38]

Congress has directed individual agencies to develop risk assessment tools and frameworks to manage and mitigate security risks. Currently, nearly each agency has developed and operates their own risk assessment tools. One such example is, as part of the Consolidated Appropriations Act of 2023,[39] Congress directed the Department of Health and Human Services (HHS) to develop a comprehensive framework and policies for assessing and managing national security risks before and after making funding awards as well as risks associated with granting access to data that may pose national security concerns.

Department of Energy

In a December 2018 memo, DOE affirmed the importance of research collaboration but raised alarms about foreign influence. The memo established a DOE S&T Risk Matrix, which identifies emerging research areas and technologies subject to restricted access by and collaboration with "sensitive country foreign nationals." The Risk Matrix is being used by the agency but is not publicly accessible. The Risk Matrix was formally codified into law with the passage of the CHIPS and Science Act. DOE also set up a Federal Oversight Advisory Body (FOAB) to

---

[33] NSF Research Security Training Modules Now available. NSF. (2024, January 30). https://new.nsf.gov/news/nsf-research-security-training-modules.
[34] NIH Advisory Committee to the Director , ACD Working Group for Foreign Influences on Research Integrity (2018). National Institutes of Health . Retrieved from https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf.
[35] U.S. Department of Health and Human Services. (n.d.). Financial conflict of interest: Investigator disclosures of foreign financial interests. National Institutes of Health. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-18-160.html.
[36] NIH, "Grants and Funding: Review Guidelines," November 19, 2020, available at https://grants.nih.gov/grants/policy/review-guidelines.htm.
[37] NIH Grants. (2020, November 9). Master class in review integrity. YouTube. https://www.youtube.com/watch?v=X0yvzUUc9yY.
[38] NSF 2022 research security training for the United States Research Community Awardees announced. NSF. (2022, December 9). https://new.nsf.gov/news/nsf-2022-research-security-training-united-states.
[39] P.L. 117-328

maintain the Risk Matrix and process exemption requests.[40] In June 2019, DOE issued a directive prohibiting DOE employees and contractors from participating in foreign talent recruitment programs sponsored by China, Iran, North Korea, and Russia.[41]

Additionally, DOE provided several other directives to continue protecting its resources. DOE has policies regarding foreign nationals' accessibility to the National Laboratories to ensure that even in an unclassified environment the federal government is protecting its investments.[42] DOE also added a requirement that anyone receiving funding from an agency must report if they have any conflict of interests that may undermine the DOE research enterprise.[43] Lastly, unlike most research agencies, DOE is a participating member of the intelligence community. This allows DOE to use unique tools to ensure its organization is secure.

RESEARCH UNIVERSITIES

The capacity to respond to research security risks varies depending on the resources, staffing, and expertise available at each institution. Some universities have set up new research security programs dedicated to identifying and mitigating risks in coordination with the IC, law enforcement, and research funding agencies. Smaller institutions are focused on raising awareness and keeping up with the patchwork of new requirements. A fall 2019 survey describes the range of activities on university campuses.[44] However, many universities are awaiting guidance from the federal government on the requirements for institutional programs to certify compliance with NSPM-33 directives, including the draft guidance OSTP noticed in the federal register in March 2023.[45] In the last 11 months, many institutions have been left in limbo and have requested OSTP hold listening sessions to receive feedback on the proposed research security programs standard guidance.[46]

---

[40] U.S. Department of Energy, UNCLASSIFIED FOREIGN NATIONAL ACCESS PROGRAM (2021). Retrieved from https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg/@@images/file.

[41] LaBarge, J. (2021, April 23). Doe O 486.1, Department of Energy Foreign Government Talent Recruitment Programs. Department of Energy Foreign Government Talent Recruitment Programs - DOE Directives, Guidance, and Delegations. https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder.

[42] Emanuelson, J. (2022, March 3). Doe O 142.3b CHG 1 (LtdChg), Unclassified Foreign National Access Program. Unclassified Foreign National Access Program - DOE Directives, Guidance, and Delegations. https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg.

[43] Ison, J. (2021, July 9). Doe O 486.1A, foreign government sponsored or affiliated activities. Foreign Government Sponsored or Affiliated Activities - DOE Directives, Guidance, and Delegations. https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder-a.

[44] University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus. (2020, May). Association of American Universities . Retrieved from https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf.

[45] OSTP, Request for Information; NSPM 33 Research Security Programs Standard Requirement, 88 Federal Register 14187, April 7, 2023, https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement.

[46] Smith , T., & Asbury , M. (2023, May 31). Request for Information; NSPM 33 Research Security Programs Standard Requirement. Association of American Universities . Retrieved from

RECENT CONGRESSIONAL ACTIONS

Over the past four years, the Science, Space, and Technology Committee has worked to address many of these research security concerns and build a more effective and resilient R&D ecosystem. This Committee has consistently strived to balance security risks and the importance of scientific openness and international collaboration. Some of the legislative actions take include:

Securing American Science and Technology Act [47] established an interagency committee within the White House Office of Science and Technology Policy (OSTP) to coordinate research security across the Federal government. It also established the National Science, Technology, and Security Roundtable at the National Academy of Sciences to facilitate collaboration between universities, federal agencies, law enforcement, and other stakeholders.

Disclosure Requirements for Federal Science Agencies

The Government Accountability Office (GAO) issued a report in December 2020 assessing the COI and disclosure policies at NSF, NIH, the National Aeronautics and Space Administration (NASA), DOD, DOE, and 11 universities.[48] GAO found that all five agencies require researchers to disclose information as part of their grant proposal but that there was variability in the policies and agencies lack clear enforcement mechanisms. GAO also concluded that, due to differing policies and inconsistent implementation, researchers may be unsure of what they need to disclose. In response, DOE established an interim COI policy on December 20, 2021,[49] and NASA updated their COI policy on August 31, 2023.[50]

In response to this report, in January 2021, as part of the NDAA for Fiscal Year 2021, Congress moved to standardize disclosure policies by mandating that each federal agency require individuals applying for federal R&D funding to disclose all current and pending research support during the application process.[51] Congress also charged OSTP, acting through the NSTC Research Security Subcommittee, with ensuring the consistency of such requirements established by federal agencies.[52]

---

https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/NSPM-33%20RSPS%20AAU%20Comments.pdf.

[47] P.L. 116-92, Div. A, Title XVII, §1746(a).

[48] U.S. Government Accountability Office, "Federal Research Agencies need to Enhance Policies to Address Foreign Influence," December 17, 2020, available at https://www.gao.gov/assets/gao-21-130.pdf.

[49] DOE, "DOE Interim Conflict of Interest Policy," https://www.energy.gov/sites/default/files/2022-10/Department%20of%20Energy%20Interim%20Conflict%20of%20Interest%20Policy.pdf.

[50] NASA, "Conflict of Interest Policy for Recipients of NASA Financial Assistance Awards," 88 Federal Register 60243, August 31, 2023, https://www.federalregister.gov/documents/2023/08/31/2023-18802/conflict-of-interest-policy-for-recipients-of-nasa-financial-assistance-awards.

[51] Section 223, National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283); 42 U.S.C. §6605.

[52] P.L. 116–283, Div. A, Title II,

CHIPS and Science Act of 2022 [53]

- Prohibits all federally funded research grantees from being a member of a malign foreign talent program or participating in similar activities.
- Prohibits federal agency personnel from participating in foreign talent programs and requires researchers working on federally funded research projects to disclose any participation in foreign talent recruitment programs.
- Requires all federally funded grantees to take annual training on research policies and foreign threats and directs OSTP to work with NSF and NIH to develop training for all grantees across the Federal research agencies.
- Directs NSF to develop a plan to identify research areas that may involve access to classified or controlled unclassified information and to exercise due diligence processes in granting access to such information.
- Bans NSF funding from going to organizations hosting Confucius Institutes.
- Creates an Office of Research Security and Policy at NSF and gives the office and the Inspector General additional resources and new authorities to use analytical tools to detect and combat foreign influence, theft, and grant fraud.
- Gives Federal research agencies the authority to require the submission of supporting documentation and the authority to act on findings that identify undue foreign influence or grant fraud.
- Directs NSF to collect annual summaries of foreign financial support from universities and grants NSF the authority to request copies of contracts or documentation related to such disclosures.
- Directs NIST to assist universities in adopting the Cybersecurity Framework to help mitigate cybersecurity risks related to conducting research. In addition, title III directs the development of a national secure computing enclaves program to protect sensitive research information at American universities from cyber theft.

[53] P.L. 117-167, Title III, Subtitle D; and Title VI, Subtitle D.