NSF SECURE Center

NSF SECURE Center

Research Security Reference Library

Updated November 17, 2025

Contents

Federal-Wide Research Security Efforts

NSPM-33 and Related Documents

1. A Presidential Memorandum on U.S. Government-Supported Research and Development (R&D) National Security Policy, known as National Security Presidential Memorandum-33 (NSPM-33) was issued by the White House Office of Science and Technology Policy (OSTP)/National Science & Technology Council's (NSTC) Research Security Subcommittee in January 2021. The stated purpose was to strengthen protections of U.S. Government-supported R&D against foreign government interference and exploitation. A focus was ensuring that recipients of U.S. federal R&D fully disclose information that can reveal potential conflicts of interest and commitment. NSPM-33 also required that research institutions receiving federal R&D funding in excess of $50 million annually certify that the institution has established and operates a research security program. Per NSPM-33 the programs will address cybersecurity, foreign travel security, insider threat awareness and identification (research security training), and, as appropriate, export control training. As of November 2025, federal agencies continue to coordinate and work to implement this requirement for awardee institutions.
2. Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise (January 2021, issued by the NSTC Research Security Subcommittee): A supplement to NSPM-33 outlining recommendations for research organizations to enhance research security and integrity. Categories include: Demonstrate organizational leadership and oversight; Establish an expectation of openness and transparency; Provide and share training, support, and information; Ensure effective mechanisms for compliance with organizational policies; and Manage potential risks associated with collaborations and data.
    a. University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus (May 2020, joint release from the Association of American Universities (AAU) and the Association of Public and Land-Grant Universities (APLU)): Provides effective practices that can be utilized by universities to implement research security efforts and minimize foreign influence.
    b. Principles and Values to Guide Actions Relevant to Foreign Government Interference in University Research (May 2021, joint release from AAU & APLU): This letter highlights key principles that can be adapted by both universities and the federal government to protect the research enterprise from foreign influence.
    c. Protect Your Organization from the Foreign Intelligence Threat (December 2021, issued by the National Counterintelligence and Security Center): The document includes links to risk mitigation materials that can be utilized to improve: physical security, personnel security, operations security, cybersecurity, defensive counterintelligence, insider threat mitigation, and supply chain risk management.
3. Guidance for Implementing NSPM-33 (January 2022, report by the White House OSTP/NSTC Research Security Subcommittee): Provides additional details on 1.) Disclosure Requirements and Standardization 2.) Persistent Identifiers 3.) Consequences for Violation of Disclosure Requirements 4.) Information Sharing and 5.) Research Security Programs (largely superseded by the final July 9, 2024 guidelines).

a. Summary of NSTC Guidance for Implementing NSPM-33 Provisions (January 2022, issued by the Council on Governmental Relations (COGR): A summary document that highlights key points of the Guidance

Common Forms for Biosketches and Current & Pending (Other) Support

1. DRAFT Research Security Programs Standard Requirement (February 2023, issued by OSTP/the NSTC Research Security Subcommittee): Draft standards for research security programs provided in this document and published for comment were superseded by the final standard guidelines published on July 9, 2024. The following are related documents and comments from higher education associations.
    a. Request for Information; NSPM 33 Research Security Programs Standard Requirement (March 2023, issued by the White House OSTP)
    b. Dear Colleague Letter (NSF 23-098) (May 2023, issued by NSF)
    c. COGR Response: Request for Information; NSPM 33 Research Security Programs Standard Requirement (May 2023, issued by COGR)
    d. Association of American Universities (AAU) Response: Re: Request for Information; NSPM 33 Research Security Programs Standard Requirement (May 2023, issued by AAU)
    e. AAMC Response: Re: Request for Information; NSPM-33 Research Security Programs Standard Requirement (88 FR 14187) (June 2023, issued by the Association of American Medical Colleges (AAMC))
    f. EDUCAUSE Response: RE: Comment on Research Security Programs (June 2023, issued by EDUCAUSE)
2. Current and Pending (Other) Support Common Form (November 2023, issued by the NSTC Research Security Subcommittee. The National Science Foundation (NSF) serves as a steward of the forms.) The common forms for federal-wide use were created as directed by NSPM-33. The form includes certification to be completed by each senior/key person at the time of submission that they are not a party to a malign foreign talent recruitment program as defined in the CHIPS and Science Act of 2022. As of November 2025, the form has been implemented by NSF and the National Aeronautics and Space Administration (NASA).
3. Biographical Sketch Common Form (November 2023, issued by the NSTC Research Security Subcommittee. NSF serves as a steward of the forms.) The common forms for federal-wide use were created as directed by NSPM-33. The form includes certification to be completed by each senior/key person at the time of submission that they are not a party to a malign foreign talent recruitment program as defined in the CHIPS and Science Act of 2022. As of November 2025, the form has been implemented by NSF and NASA.
4. NSPM-33 Implementation Guidance Appendix: Definitions (November 2023): Supplement to NSPM-33 Implementation Guidance that provides definitions of terms.
5. NSTC Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support (Last updated May 2024): A matrix developed to assist in determining if specific activities are required to be disclosed and what form is appropriate for reporting.

6. Policy Regarding Use of Common Disclosure Forms for the "Biographical Sketch" and the "Current and Pending (Other) Support" Sections of Applications by Federal Research Funding Agencies (February 2024: Issued by the White House OSTP): Requires federal agencies to use the Common Forms for current and pending support and biosketches and notes that NSF will serve as steward. Deviation from the common disclosure forms will require Office of Management and Budget (OMB)/Office of Information and Regulatory Affairs (OIRA) review and clearance under the Paperwork Reduction Act (PRA).
7. Final Guidelines for Research Security Programs at Covered Institutions - Final Research Security Program (RSP) Guidelines were published on July 9, 2024, via this memorandum to the heads of federal research funding agencies issued by the White House OSTP. Federal agencies are directed to implement the guidelines and provide time for institutional implementation. A summary of the guideline requirements in the four required areas can be found below. A summary of the guideline requirements in the four required areas, published in COGR's July 2024 overview, can be found below..

Agencies are coordinating implementation of the RSP requirements under a memorandum of agreement and anticipated to issue the requirements in early 2026.

8. Research Security Training was developed by institutions and organizations under cooperative agreements funded by NSF in collaboration with the National Institutes of Health (NIH), Department of Energy (DoE) and Department of Defense(DoD), with engagement from the Federal Bureau of Investigation (FBI). The training consists of 4 modules: 1.) What is Research Security?; 2.) Disclosure; 3.) Manage and Mitigate Risk; 4.) International Collaboration.
    a. The SECURE Center offers an updated one-hour condensed and consolidated federal research security training module, CTM 1.1. NSF, NIH, DoD, DOE and USDA have indicated that the condensed module meets their research security requirements. The SCORM files (for upload in the institution's learning management systems), Storyline file, and transcript can also be found here. The training includes two, four or six editable html-based files that can be modified to supply institution-specific contact information and

links to resources. A preview version can be viewed on the website and a version of the training that offers a certificate of completion is now available.

   b. The University of Michigan, in collaboration with the Ohio State University, Stanford University, and Duke University, developed a condensed and consolidated one-hour version of the four federal training modules that other academic institutions or organizations can download for their use. This training includes two editable html-based files that can be modified to supply institution-specific contact information and links to resources. The SCORM files (for upload in the institution's learning management systems), Storyline file, and written version of the narrative can be found here.

9. Cybersecurity for Research: Findings and Possible Paths Forward-NIST 8481 (August 2023, issued by the National Institute of Standards and Technology (NIST)). This is an initial public draft that summarizes feedback NIST received on institutions of higher education (IHE) cybersecurity challenges and includes resources and possible next steps. Per the final research security program guidelines published July 9, 2024, institutions are to implement a cybersecurity program one year after publication of the final version of this NIST cybersecurity resource. However, federal research funding agencies, working with NIST and IHEs via the Federal Demonstration Partnership (FDP) are currently developing cybersecurity guidelines that align with NIST 8481 for use in RSPs.
10. Safeguarding International Research (NIST IR 8484) (August 2023, issued by NIST): Integrates several U.S. government policies and guidelines to develop a framework for an integrated, risk-balanced approach for safeguarding international science and technology from undue foreign interference.
11. Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs (February 2024, issued from the White House OSTP): Per Section 10631 of the CHIPS and Science Act, this document provides definitions of both foreign talent recruitment program (FTRPs) and malign foreign talent recruitment programs (MFTRPs) [pages 4-6] and what is not considered an FTRP. A foreign talent recruitment program is any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.
12. Critical and Emerging Technologies List (February 2024, a report from the Fast Track Action Subcommittee on Critical and Emerging Technologies of the NSTC): This biannual update defines critical and emerging technologies (CETs), which are a subset of advanced technologies that have a significant impact on U.S. national security. [List of CETs is outlined on pages 8-11]
13. ADVANCING INTERNATIONAL COOPERATION IN QUANTUM INFORMATION SCIENCE AND TECHNOLOGY (August 2024, Issued by Subcommittee on Quantum Information Science, Committee on Science, NSTC): This report emphasizes the importance of the critical quantum information science and technology (QIST) field and the need to enhance interagency cooperation, fund international collaboration, and track global competitiveness.

14. Actions Taken to Address Foreign Security Threats, Undue Foreign Interference, and Protect Research Integrity at U.S. Universities (AAU, updated in January 2024): A summary document that references key federal documentation that has been developed to address foreign influence in research.
15. Quick Reference Table of Current & Upcoming Federal Research Security Requirements (September 30, 2025, updated by COGR): A matrix that lists policies and requirements under the headings of: Disclosures, Agency Risk Assessment, FCOI & COC, Training, Certifications, and Research Security Program for each federal agency. Per COGR, this tool is frequently updated to reflect the release of new documentation.
16. Matrix of Science & Security Laws, Regulations, and Policies (September 30, 2025, updated by COGR): A chart that compares federal laws, regulations, and policies in the area of science and security. The chart is divided into three separate tabs that cover (a) major federal-wide legislation or policy, (b) agency disclosure requirements for researchers and research institutions; and (c) agency conflict of interest policies.

Research Security Legislative Requirements and Congressional Activities

National Defense Authorization Act (NDAA)

1. Research Security Requirements in Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) (signed into law July 26, 2018):
   Section 1286 directs the Secretary of Defense to establish an initiative to work with IHEs who perform defense research and engineering activities and name an academic liaison. It also directed DoD to publish a list of institutions and foreign talent recruitment programs that have perpetuated malicious activities or that "operate under the direction of the military forces or the intelligence agency of the applicable country and thus pose a threat to national security." The resulting list is updated annually, the reference below is the current list.
2. Introduction to FY23 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended (June 24, 2025, by the DoD)
3. FY20 NDAA (December 20, 2019, U.S. Congress)
   Section 1746 directs OSTP to establish an interagency working group (the Research Security Subcommittee) under the NSTC to protect federally funded R&D from foreign interference, cyberattacks, theft, or espionage and to develop recommendations for best practices for federal agencies and grantee institutions. The working group was established in May 2019.
   Section 1746 called on the National Academy of Science, Engineering and Medicine to stand up a new Roundtable on Science, Technology, and Security to bring together key stakeholders from the scientific enterprise (including federal agencies, universities, and industry) to enter into a constructive and ongoing dialogue on research security.The Roundtable Capstone report can be found here.
   Confucius Institutes at U.S. Institutions of Higher Education: Waiver Criteria for the Department of Defense (January 2023, issued by the National Academies) Summary that outlines recommended conditions that should be in place for DoD to consider granting a waiver to allow an IHE hosting a Confucius Institute (CI) to continue receiving agency funding.
4. FY21 NDAA (January 3, 2020, U.S. Congress)
   Section 223 mandates disclosure of funding sources in applications for federal R&D awards. Additionally, universities are held accountable for ensuring faculty are aware of these disclosure requirements.
   Section 1299C is an amendment to FY 2019 NDAA Section 1286 requiring designation of an official responsible for liaising with academic institutions and briefing them on espionage risks.
   Section 1062 restricts DoD and NSF funds to institutions that host a Confucius Institute.
   Section 9907 prohibits any funds appropriated for its microelectronics initiatives and incentives to be provided to a "foreign entity of concern," defined broadly, to include nationals of certain countries.

CHIPS and Science Act Research Security Highlights

1. CHIPS and Science Act (August 2022, includes a number of research security provisions, some of which are included below):
    a. **Sec. 10114. Research Security –** DOE Office of Science to develop and maintain tools and processes to manage and mitigate research security risks such as an S&T risk matrix, informed by threats identified by the Office of Defense National Intelligence (ODNI).
    b. **Sec. 10228. Protecting research from cyber theft –** Requires NIST to consider the needs of IHEs when creating cybersecurity guidance.
    c. **Sec. 10229. Dissemination of resources for research institutions –** Requires NIST to offer resources and technical assistance to research intensive universities to help them mitigate cyber risks related to conducting research.
    d. **Sec. 10331. Office of Research Security and Policy –** Establishes an Office of Research Security, Strategy, and Policy within NSF.
    e. **Sec. 10332. Chief of Research Security –** Establishes a Chief of Research Security position within the NSF Office of the Director to manage the Office of Research Security and Policy.
    f. **Sec. 10334. Online resource –** Directs [NSF] to develop an online resource to inform institutions and researchers of security risks and best practices and explain Foundation research security policies.
    g. **Sec. 10336. Authorities –** Authorizes the NSF OCRSSP, in coordination with the Office of Inspector General (OIG), to conduct risk assessments, including through the use of open-source analysis and analytical tools, of R&D award applications and disclosures to NSF.
    h. **Sec. 10337. Responsible conduct in research training –** Expands the requirement for RCR training to include faculty and other senior personnel on [NSF] awards and expands the scope of such training to include mentoring training and training to raise awareness of research security risks as well as Federal export control, disclosure, and reporting requirements.
    i. **Sec. 10338 - Research security and integrity information sharing analysis organization –** Directs [NSF] to establish a research security and integrity information sharing analysis organization to enable the research community to share information, identify research security risks, and implement risk assessment and mitigation best practices and procurement of a non-government organization to run this center. The SECURE Program, including the SECURE Center and SECURE Analytics, were implemented to answer this call.
    j. **Sec. 10339A. Foundation funding to institutions hosting or supporting Confucius institutes –** Places restrictions on eligibility for NSF R&D funding for institutions that host or support Confucius [or Confucius-like] institutes.
    k. **Sec. 10339B. Foreign financial support –** Directs NSF to collect annual summaries of foreign financial support from universities. The provision establishes a reporting threshold of $50,000 or more in [cumulative] financial support, including gifts and contracts, received directly or indirectly from a foreign country of concern (China, Russia, North Korea, and Iran at the time the law was enacted), or any other country determined to be a concern by

the Secretary of State. This is in addition to the reporting of gifts and contracts from all foreign countries with a cumulative value of $250,000 or more via the Higher Education Act and Department of Education.

l. **Sec. 10631. Requirements for foreign talent recruitment programs –** OSTP to issue guidance to Federal research agencies to prohibit participation in "foreign talent recruitment programs" by agency personnel and provide additional clarification to the research community regarding which activities are considered "foreign talent recruitment programs." OSTP is also directed to issue guidance clarifying that researchers working on Federally supported research projects must disclose participation in FTRPs in Federal research award proposals. OSTP is further directed to issue guidance for Federal research agencies to prohibit researchers working on agency-funded projects from participating in "malign foreign talent recruitment programs," and certify both at the time of proposal and annually that they are not part of a malign foreign talent recruitment program.

SBIR and STTR Extension Act of 2022

1. SBIR and STTR Extension Act of 2022 (September 2022) Requires agencies to implement a due diligence program to assess security risks for SBIR and STTR proposals. Disclosure requirements include information on foreign ties, business relationships, investment, and ownership [Source: AAU, January 2024].

Congressional Activities & Resources

1. House committee on Science, Space and Technology hearing "Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise" with representatives from the White House (OSTP), NSF, NIH and DoE (Hearing held in February 2024)
2. Federal Research Security Policies: Background and Issues for Congress (May 20, 2025): The Congressional Research Service (CRS) issued a report on May 20, 2025, summarizing federal research security policy efforts to date, and providing options Congress might consider to address perceived gaps or deficiencies while also remaining cognizant of the potential increase to administrative burden they would present.
   Proposed options discussed include:
   a. Expanding sources of foreign support researchers are required to disclose beyond those that involve the design, conduct or reporting of research,
   b. Broadening the scope of who is required to disclose Current and Pending (Other) Support (i.e., beyond senior/key personnel),
   c. Increasing the frequency of post-award updates to Current and Pending (Other) Support,
   d. Expanding agency requirements when reviewing disclosed information to include the identification of potential security vulnerabilities,
   e. Focusing risk assessment activities more narrowly (e.g., increasing focus on research involving critical and emerging technologies),
   f. Expanding agencies' requirements to report to congress on: research security violations; mitigation measures required; status of the implementation of requirements; or tasking a nongovernmental entity (e.g., the SECURE Center) with compiling this information to report to Congress

Research Security-Related Reports

1. Fundamental Research Security JSR-19-21 (December 2019, a report from the JASON Group commissioned by NSF): The report outlines that concerns of foreign influence can be addressed within the framework of research integrity and, in addition, that the benefits of openness in research and of the inclusion of foreign researchers dictate against measures that would restrict fundamental research. **The report includes questions for researchers to consider when entering a collaboration [Section 7.3 Assessment Tools: pages 34-36].**
    - National Science Foundation Response to the JASON Report 'Fundamental Science and Security'
2. Safeguarding the Research Enterprise (JSR 23-12) (March 2024, commissioned by NSF and issued by the JASON group): Recommends NSF adopt a dynamic approach for identifying potentially sensitive research topics as they arise and weigh the balance between the positive protective benefits and the unintended negative consequences of controls on sensitive research. It is suggested that the identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the institution and be proportionate to the assessed risk, relative to the associated costs.
3. Foreign-Funded Language and Culture Institutes at U.S. Institutions of Higher Education: Practices to Assess and Mitigate Risk (June 2023, issued by the National Academies) Summary providing recommendations that U.S. institutions of higher education can take to identify and mitigate risks associated with foreign-funded language and culture institutes on campus.
    - RULES COMMITTEE PRINT 118–46 TEXT OF H.R. 1516, DHS RESTRICTIONS ON CONFUCIUS INSTITUTES AND CHINESE ENTITIES OF CONCERN ACT (September 2024, report ordered by Committee on Homeland Security): States that IHEs which have a relationship with a Confucius Institute or Chinese entity of concern is ineligible to receive any funds from the Department of Homeland Security, unless the institution terminates the relationship.
4. International Talent Programs in the Changing Global Environment (2024, National Academies: Sciences, Engineering and Medicine)
5. Responsible Collaboration Through Appropriate Research Security: A Workshop To Discuss and Study the Emergent Discipline of Research on Research Security (RoRS) (2024, Rice University, commissioned by NSF) A summary of the NSF-funded workshop "Responsible Collaboration Through Appropriate Research Security" held at Rice University's Baker Institute for Public Policy in May 2024. Discusses challenges and opportunities in the emerging field of RoRs and provides recommendations to guide NSF's new RoRS program.
6. The National Academies of Sciences, Engineering, and Medicine's National Science, Technology, and Security Roundtable, called for in the Fiscal Year 2020 National Defense Authorization Act, explored issues related to protecting U.S. national and economic security while ensuring the open exchange of ideas and the international talent. A capstone report can be found here
7. A National Academies Committee published the report, *Simplifying Research Regulations and Policies: Optimizing American Science* on September 3, 2025. The Committee "conducted an expedited study to examine federal research regulations and identify ways to improve regulatory processes and administrative tasks, reduce or eliminate unnecessary work, and modify and remove policies and regulations that have outlived their purpose while maintaining necessary and

appropriate integrity, accountability, and oversight. The report covers the broad landscape of research administration and compliance. Research security specific options include:

- Implement the National Security Presidential Memorandum-33 (NSPM-33) common disclosure forms and disclosure table, without deviation, as the primary means to identify and address Conflicts of Commitment (COCs) and develop federal-wide FAQs via the interagency working group; in addition, use the Science Experts Network Curriculum Vitae (SciENcv) system, persistent identifiers (PIDs), and application programming interfaces (APIs) across research funding agencies.
- Establish common principles for agency research security risk reviews for fundamental research.
- Continue prior efforts, chiefly the Export Controls Reform Initiative, to streamline and clarify export controls and reduce associated administrative work, with representation from the academic research community and expedite licensing processes for low-risk, controlled research.
- Adapt cybersecurity requirements for university settings: direct NIST (National Institute of Standards and Technology], in collaboration with OSTP and the broader research community, to undertake a comprehensive review of cybersecurity controls as they apply to institutions of higher education and make appropriate modifications to ensure alignment with the academic research environment.

8. The National Academies *Assessing Research Security Efforts in Higher Education* working group held a number of meetings and a May workshop with federal and non-federal experts beginning September 2024 and concluding September 4, 2025, to discuss assessment of federal research security efforts. Proceedings from the workshop can be found here.

Federal Agency-Specific Research Security Policies, Requirements, and Resources

Department of Defense (DoD)

1. Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education (June 29, 2023, issued by DoD): The document includes:

1. A *Policy on Risk-based Security Reviews of Fundamental Research*,
2. A *Decision Matrix to Inform Fundamental Research Proposal Mitigation* (Amended May 5, 2025),
3. A list of foreign institutions identified as engaging in problematic activity (Part 3, Table 1 (Amended June 24, 2025)., and
4. A list of foreign talent recruitment programs identified as posing a threat to U.S. national security interests (Part 3, Table 2).

   The policy is part of the Department's effort to counter unwanted foreign influence in, and misappropriation of, DoD-funded research to the detriment of national or economic security. The Decision Matrix contains four factors for assessing senior/key personnel disclosures:

   a. Participation in foreign talent recruitment programs
   b. Current or prior funding from "foreign countries of concern" (FCOCs). FCOCs are currently defined as China, Russia, North Korea, and Iran per section 10612 of the CHIPS Act of 2022.
   c. Filing a patent in an FCOC or on behalf of an FCOC-connected entity, or in a non-FCOC country without disclosure, and
   d. Associations or affiliations with organizations on U.S. Entity (trade restriction) and other indicated (U.S. restricted) lists.

   The policy document and matrix serve as a guide to assist DoD program managers in reviewing fundamental research (that is, not classified or controlled unclassified) proposals selected for award for potential conflicts of interest and commitment using information disclosed by senior/key personnel. Per DoD, updates to the matrix will be made available on DoD's Basic Research webpage.

   a. Survey on Research Institutions' Experiences with DoD Policy for Risk-Based Security Reviews of Fundamental Research (April 2024, issued by COGR)

   b. Defense Advanced Research Projects Agency (DARPA) Fundamental Research Risk-Based Security Review Program (FRR-BS) Frequently Asked Questions (FAQs) (May 2024)

5. Final Cybersecurity Maturity Model Certification (CMMC) Program (32 CFR 170) (October 2024, DoD Office of the Secretary)

   a. Supplemental summary document, press release from the DoD
   b. Cybersecurity Maturity Model Certification (CMMC) Program proposed rule (December 2023, issued by the Department of Defense (DoD) Office of the Secretary)

   c. RE: Comments in response to Docket Number DoD–2023–OS–0063 / Regulatory Identifier Number (RIN) 0790–AL49, "Cybersecurity Maturity Model Certification (CMMC) Program.": Issued by ACE, AAU, APLU,COGR, EDUCAUSE on February 26, 2024

6. DoD published Fundamental Research Guidance on August 4, 2025. The Guidance provides background on Fundamental Research (FR) as defined by NSDD-189 and DoD's implementation of the Directive via the May 24, 2010 "Carter Memo". The Guidance notes that "under the Carter Memo, research funded by 6.1 budget activity or 6.2 research conducted on a university campus is fundamental. For other research categories, the Department must be deliberate when deciding that a particular research topic is appropriate for openly published fundamental research". It incorporates Considerations for Program Managers and Contracts and Grants Officers, including:
   a. Refraining from imposing publication review of research that has been formally designated as fundamental;
   b. For awards with multiple performers, considering whether some portion of the work should be designated as FR even if much of the award is not; and,
   c. Avoiding flowing down restrictions to awardees performing FR that are inappropriate for FR.

   In addition, apart from Risk-Based Security Reviews of Fundamental Research, that no security vetting should be done on personnel engaged in fundamental research and "no preapproval conditions for the addition of researchers such as students, postdoctoral fellows, laboratory technicians, or other persons not labeled as senior/key personnel by the research performer should be placed on awards for fundamental research." Considerations for Prime Awardees include that in cases where a subawardee requests a FR designation, prime awardees are encouraged to contact the Program Manager and request such a designation. Taken together, the guidance has the potential to (1) Significantly limit restrictions on fundamental research that can preclude the participation of some institutions and (2) Foster the open exchange of scientific information.

7. DoD Publishes Federal Rule for DFARS CMMC 2.0 Standards: In the September 10, 2025, Federal Register, the Department of Defense (DoD) issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the final Cybersecurity Maturity Model Certification (CMMC) program rule. The new rule formalizes the ability of the DoD to include CMMC requirements as a condition of contract award, to include either Federal Contract Information (FCI), Controlled Unclassified Information (CUI), or both.

National Aeronautic and Space Administration (NASA)

1. Appropriations Law (Section 1340 of Public Law 112-10, aka, the "Wolf Amendment," 2011): Prohibits participation, collaboration, or coordination bilaterally with China or any Chinese-owned company on any NASA project at the prime or subrecipient level. In a September 2022 presentation (49:32 in the video), NASA clarified that the agency defines a 'Chinese-owned company' as any company owned by China, or any company incorporated under the laws of China, and that Chinese universities and similar institutions are considered to be incorporated under the laws of China and therefore the funding restrictions apply.
2. Proposer's Guide (February 2023): Includes similar language to the above in a footnote of section 2.16, Current and Pending Support. Per the footnote, "'China or Chinese-owned Company' means

the People's Republic of China (PRC), any company owned by the PRC, or any company incorporated under the laws of the PRC. Chinese universities and other similar institutions are considered to be incorporated under the laws of the PRC and, therefore, the funding restrictions apply to grants and cooperative agreements that include bilateral participation, collaboration, or coordination with Chinese universities."

Department of Energy (DoE)

1. Department of Energy Financial Assistance Letter (FAL): Digital Persistent Identifier Requirements for Certain Individuals for Research and Development (Issued on August 8, 2024): Effective May 1, 2025, applicants are required to have a Digital Persistent Identifier or Persistent Identifier (PID) if: 1. Individuals are listed within financial assistance applications that will fund R&D activities, or technical assistance to support R&D activities; and 2. Individuals are required to submit Biographical Sketch and/or Current and Pending (Other) Support disclosure.
   A PID is defined as *globally unique, persistent, machine resolvable and processable, and has an associated metadata schema* (example: ORCID iD). PIDs must be provided in the Biographical Sketch and/or Current and Pending (Other) Support disclosures as part of the application. This requirement is optional until May 1, 2025, and mandatory thereafter.

2. Department of Energy Financial Assistance Letter (FAL): Research Security Training Requirements for all R&D Financial Assistance Awards (Issued on October 7, 2024)
   This document outlines DOE's implementation of research security training requirements for covered individuals on financial assistance applications and for organizations applying for an award. The requirement was effective immediately but not mandatory until May 1, 2025. The training requirement is satisfied either by completion of the four training modules created by NSF, completion of the SECURE Center CTM (as indicated per DOE post FAL), or by a custom training program that is aligned with the CHIPS and Science Act Section 10634(b). Per DOE the training must be completed within the 12 months immediately preceding the application submission, consistent with the CHIPS Act requirements, and any covered individuals added to the project must certify that they have completed the training within 30 calendar days of joining the project.

3. DOE Research, Technology, and Economic Security (RTES) Framework for Financial Assistance and Loan Activities (Issued on November 26, 2024) DOE's RTES office issued a "framework to minimize, mitigate, and manage risks while maintaining an open, collaborative, and world-leading scientific enterprise." The process includes three phases during which RTES will coordinate with program offices. This includes ensuring solicitations include appropriate language on RTES requirements, including assessment of technology risk level; and RTES "due diligence" reviews before selection for award; and changes that occur during the life of a project that may trigger RTES review.
   Risk reviews use information disclosed to the agency as well as public and classified sources. Risk factors include ties to malign foreign talent recruitment programs, "certain foreign funding sources", "certain concerning behaviors associated with patenting" (e.g., transferring to foreign entities after filing), and ties to foreign entities or foreign collaborators on specified [certain U.S. restricted] lists "or with specified characteristics."
   a. RTES presented on research security risk reviews during a COGR meeting in October 2023, noting that much of the agency's portfolio includes critical and emerging

technologies. Among the areas noted as potential targets were Advanced batteries, Advanced computing, Advanced engineering materials, Advanced manufacturing, Artificial intelligence/machine learning, Autonomous systems and robotics, Biotechnologies, Quantum information technologies, Next generation renewable energy generation and storage and Semiconductors and microelectronics.

4. Transparency of Foreign Connections Disclosure and Certification: For applicants, recipients, and subrecipients that are required to submit transparency of foreign connections disclosures, DOE provides this format for the convenience of the entity providing the disclosure and certification; however, the entity is not required to use this specific format. If another format is used, the signatory must include the same substantive information, a signature, date, and the certification statement provided in Section 3 of the document.

National Institute of Health (NIH)

1. Reminders of NIH Policies on Other Support and on Policies related to Financial Conflicts of Interest and Foreign Components (NOT-OD-19-114) (July 10, 2019): Reminds institutions receiving NIH funding of the requirement for researchers to disclose *all* sources of support for their research endeavors, regardless of the source, value, or whether monetary or in-kind, and to disclose all scientific appointments and positions, whether foreign or domestic, paid or unpaid, etc. The notice also reminds the extramural community of the requirement to comply with HHS regulations regarding Financial Conflicts of Interest, as well as the requirement to report all Foreign Components involved in NIH-supported activities.
2. Upcoming Changes to the Biographical Sketch and Other Support Format Page for Due Dates on or after May 25, 2021 (NOT-OD-21-073) (March 2021): Requires immediate notification of undisclosed Other Support. If a recipient discovers Other Support information on an active NIH grant that should have been, but was not, disclosed during just-in-time or in an annual progress report, updated Other Support must be submitted to the Grants Management Specialist as soon as the undisclosed information is known.
3. NIH Decision Matrix for Assessing Potential Foreign Interference for Covered Individuals or Senior/Key Personnel (August 2024): Assists agency staff in assessing grant applications and ongoing awards for potential foreign interference. Factors considered include: (1) current or past participation in a malign foreign talent recruitment program, which is prohibited by law, (2) undisclosed current or prior funding from a foreign country of concern (FCOC), or connected entity (currently China, Russia, North Korea, and Iran (higher risk)) or other foreign country (lower risk) and, (3) Indicators of an undisclosed current or past affiliation with an institution or entity located in or connected to a FCOC (higher-risk/mitigation) or foreign country (lower-risk/mitigation). Per the matrix, mitigation is either required, recommended, suggested, or not required based on the timing of the engagement (active/current vs. within the past 5 years) and if accurate and complete disclosure information was provided. In circumstances where mitigation is required, some conditions that could be implemented include: (1) specific award conditions, (2) modification of terms and conditions of award, (3) suspension, termination, or withdrawal of an award, (4) conversion from advance payment to reimbursement, and (5) recovery of funds.

   a. NIH Blog Post (August 2024) New Decision Matrix Further Clarifies NIH Processes for Handling Allegations of Foreign Interference

4. Notice of Information: NIH SBIR and STTR Foreign Disclosure Post-Award Requirements for Active SBIR and STTR Awardees (NOT-OD-25-102) (April 29, 2025): Effective immediately the SBIR and STTR Foreign Disclosure and Risk Management Requirements described in NOT-OD-23-139 and NOT-OD-24-029 may be applied to all active SBIR and STTR awards regardless of the due date the competing application was submitted. Recipients with active awards that did not undergo foreign risk assessment at the time of their original application may be required to disclose all funded and unfunded relationships with foreign countries, using the Required Disclosures of Foreign Affiliations or Relationships to Foreign Countries Form.
   If the recipient reports a covered foreign relationship that meets any of the risk criteria prohibiting funding, NIH may deem it necessary to terminate the award for material failure to comply with the federal statutes, regulations, or terms and conditions of the federal award.

5. Updated NIH Policy on Foreign Subawards (NOT-OD-25-104) (May 1, 2025): Prospectively updates NIH policies and practices for utilizing foreign subawards. Per the notice, "NIH is establishing a new award structure that will prohibit foreign subawards from being nested under the parent grant. This new award structure will include a prime [with independent linked awards] that will allow NIH to track the project's funds individually while scientific progress will be reported collectively by the primary institution under the Research Performance Progress Report." The guide notice indicates that "NIH anticipates implementing the new award structure by no later than September 30, 2025, prior to Fiscal Year 2026." The policy further indicates that "NIH continues to support direct foreign awards" and plans to expand this policy to domestic subawards in the future, for consistency.

6. NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements (NOT-OD-25-133) (July 17, 2025): Effective October 1, 2025, recipient institutions must train senior/key personnel on the requirement to disclose all research activities and affiliations in Other Support and maintain a "written and enforced policy on requirements for the disclosure of other support to ensure Senior/Key Personnel fully understand their responsibility to disclose."

7. Updated Implementation Guidance of NIH Policy on Foreign Subawards for Active Projects (NOT-OD-25-130) (July 18, 2025): In follow-up to NOT-OD-25-104, this updated guidance creates an alternative, short-term approach for existing grants and cooperative agreements involving human subjects research (e.g., clinical trials and clinical research) with foreign sites. The alternative approach involves removing a foreign sub-award from the primary award and having it issued as a foreign supplement award.

8. Preview of NIH Common Forms for Biographical Sketch and Current and Pending (Other) Support Available in SciENcv: On September 4, 2025, the National Institutes of Health (NIH) issued notice NOT-OD-25-152, regarding the agency's plans to release preview versions of NIH's Common Forms for Biographical Sketches (Biosketches) and Current and Pending (Other) Support in the Science Experts Network Curriculum Vitae (SciENcv) system. Access to the preview versions is purely for informational purposes and applicants/recipients may not submit documents to NIH that were created using the preview functionality. Applicants/recipients must continue to use the current NIH Biosketch and Other Support forms until NIH officially implements its Common Forms,

which the agency anticipates will occur in November 2025. The fall 2025 government shutdown may impact this timeline.

9. New Application Structure for NIH-Funded International Collaborations: On September 12, 2025, the National Institutes of Health (NIH) issued NOT-OD-25-155, "New Application Structure for NIH-Funded International Collaborations," providing additional information on the agency's new process for handling foreign components, as NIH announced in NOT-OD-25-104 that the agency would not issue awards for proposals that include subawards to foreign entities.

   Under the process described in NOT-OD-25-155, competing applications that include one or more foreign components must submit to a Notice of Funding Opportunity (NOFO) that supports a complex mechanism activity code, including two new international project "parent" activity codes that NIH is creating: PF5 for grants and UF5 for cooperative agreements.

   a. On September 18, 2025, NIH released additional information regarding the agency's new application and award structure for international collaborations, previously announced in NIH NOT-OD-25-155. In addition to summarizing impacts to proposing/recipient institutions, the announcement provides links to additional information for the four new Activity Codes (grant types) that will be used to facilitate the new application and award process.

10. Required Security and Operational Standards for NIH Controlled-Access Data Repositories: On September 24, 2025, and effective immediately, NIH issued NOT-OD-25-159, establishing new security, operational, and transparency standards for controlled-access data repositories (CADRs) that store and manage sensitive human research data.

11. NIH Policy on Enhancing Security Measures for Human Biospecimens: Issued September 24, 2025, and effective October 24, 2025, NIH implemented NOT-OD-25-160, a policy to enhance security for human biospecimens in NIH-funded research.

12. Update: NIH Rescinds Notice on Implementation of Research Security Policies: In a September 29, 2025, notice (NOT-OD-25-161), the National Institutes of Health (NIH) rescinded the September 11, 2025, notice (NOT-OD-25-154) Implementation of NIH Research Security Policies. Per the notice, "NIH continues to work with the National Science Foundation and other Federal research agencies to finalize guidance on each of the required elements outlined in the Office of Science and Technology Policy (OSTP) Guidelines for Research Security Programs at Covered Institutions, and to develop a centralized process for recipients to certify compliance." The notice indicates that the implementation date for the requirements announced in NOT-OD-25-154 have not been finalized, the notice is therefore rescinded, and that "NIH will issue updated guidance on Research Security requirements in the coming months."

National Science Foundation (NSF)

1. Proposal and Award Policies and Procedures Guide (NSF 23-1) (January 2023) Post-award Disclosure of Current Support and In-Kind Contribution Information: PAPPG Chapter II.D.2.h(ii)

2. NSF Guidelines for Research Security Analytics (February 2023): Outlines advanced monitoring and verification activities of NSF proposals and awards. The guidelines largely serve to provide

transparency and identify guardrails NSF has put in place around the use of data analytics to monitor and validate information disclosed (e.g., in biosketches and current and pending support). For example, the activities are not investigative and cannot be incorporated into the merit review process. Sources of information include SCOPUS, Web of Science, and the U.S. Patent and Trademark Office Patent Database.

3. Research Program on Research Security (March 2023, report issued by JASON and commissioned by NSF): Provides definitions of Research Integrity as adherence to accepted values and principles — objectivity, honesty, openness, accountability, fairness, and stewardship — that guide the conduct of research and recognize the expectations of funding agencies, research institutions, and the research community. Research Security is protecting the means, know-how, and products of research until they are ready to be shared. JASON suggests research security does not vary across disciplines, but the consequences of breaches in research security and the measures taken to prevent breaches will differ.
   Key points include an emphasis on training researchers on risks in international collaborations, the need to encourage collaboration with international organizations that are also concerned with research security and avoiding creating a reputation of racial profiling or using the research security programs to disadvantage anyone based on ethnicity or nationality.

4. Trusted Research Using Safeguards and Transparency (TRUST) (June 2024)
   NSF initiated a proposal risk review process similar to that of DoD but with some notable differences. NSF's process will focus on critical technologies, beginning with a pilot of quantum proposals in FY25, expanding to other key technologies in phase 2, and scaling up for all key technologies identified in the CHIPS and Science Act in phase 3.
   NSF will evaluate Three Criteria: 1. Appointments and positions with U.S. proscribed parties (e.g., U.S. BIS Entity List) and currently party to a MFTRP; 2. Non-disclosures of appointments, activities, and financial support; and 3. Potential foreseeable national security applications of the research. NSF will consider only current foreign appointments and affiliations and is not considering co-authorship in risk assessment.
   Additional information presented at Federal Demonstration Partnership (FDP) Meeting in May 2024

5. Important Notice No. 149 (July 10, 2025): Includes NSF implementation of three new requirements (and three existing ones) in alignment with the CHIPS and Science Act and NSPM-33. The requirements, effective October 10, 2025, include:
   a. Recipient institutions must maintain supporting documentation for foreign activities reported as current and pending (other) support,
   b. Senior/key personnel must certify they have completed research security training (RST) within 12 months prior to proposal submission; Recipient institutions' Authorized Organizational Representative (AOR) must certify that all senior/key personnel have completed required RST and that the institution has a plan to provide appropriate training and oversight in the responsible and ethical conduct of research that meets the CHIPS Act requirements.
   c. AORs at institutions of higher education (IHEs) must certify that, absent a waiver granted by the NSF Director, the IHE does not maintain a contract or agreement between the institution and a Confucius Institute.

d. NSF Annual Malign Foreign Talent Recruitment Program Certification for PIs/co-PIs: The CHIPS and Science Act of 2022 directs federal research funding agencies to establish a policy that requires each covered individual (CI) listed in an R&D proposal to certify that they are not a party to a MFTRP in the proposal submission and annually thereafter for the duration of the award. NSF was the first federal agency to implement this certification via the common federal biosketch and current and pending support forms in May 2024. NSF began rolling out the annual certification on June 7, 2025, for all PIs and co-PIs named on an NSF award made on or after May 20, 2024. NSF is making sample contracts available that meet the parameters of a MFTRP. Contract examples and frequently asked questions can be found on the NSF website here under MFTRPs.

United States Department of Agriculture (USDA)

1. America First Memorandum for USDA Arrangements and Research Security (July 8, 2025):
    a. Requires all USDA Mission Areas, Agencies, and Offices to:
        i. Within 30 days, conduct a comprehensive review of all current USDA awards/subawards with foreign persons/entities and provide justification as to why a US recipient was not selected.
        ii. Effective immediately, request approval (including justification) prior to issuing an award/subaward to a foreign person/entity.
    b. Requires applicants (i.e., covered individuals) to
        i. Complete the Common Forms for Biographical Sketches and Current and Pending (Other) Support and provide updated information annually throughout the duration of the award.
        ii. Certify they are not a participant in a malign foreign talent recruitment program (MFTRP) and recertify annually.
        iii. Certify that they are not contracting with or providing benefit to any foreign person/entity in a country of concern.
        iv. Certify that they are not party to utilizing forced labor, or partnering with universities who are party to utilizing forced labor.
        v. Complete an annual disclosure of contracts associated with participation in programs sponsored by foreign governments/entities.
        vi. Seek approval from USDA to subaward any portion of a funded arrangement, including but not limited to university students, post-doctoral fellows, and visiting researchers.
    c. Requires Employing Entities to:
        i. Certify to applicants' completion of research security training and awareness of the requirements.
        ii. Prohibit applicants who either are currently or have in the past 10 years participated in malign foreign talent recruitment programs (MFTRPs) from working on projects supported by USDA Research and Development or Science and Technology awards.
        iii. Provide supporting documentation (e.g., contracts) for foreign activities reported as current and pending support

iv. Review any documents required under the memorandum for compliance with USDA award terms and conditions, including guidance on conflicts of interest and conflicts of commitment.

Useful Links

1. Office of the Director of National Intelligence (ODNI): Research Security
2. National Science Foundation (NSF): Research Security
3. National Institute of Health (NIH): Foreign Interference
4. Department of Energy (DOE): Research, Technology & Economic Security
5. Department of Defense (DOD): Basic Research/Research Directorate
6. Association of American Medical Colleges (AAMC): Research Security and Foreign Influence at U.S. Academic Institutions
7. Council On Governmental Relations (COGR): COGR Homepage
    - Matrix of Science & Security Laws, Regulations, and Policies
    - Quick Reference Table of Current & Upcoming Federal Research Security Requirements
8. Federal Demonstration Partnership (FDP): FDP Homepage
9. Association of American Universities (AAU): AAU Homepage
10. Association of Public & Land-Grant Universities (APLU): APLU Homepage

Historical Documents

1. National Security Decision Directive-189: National Policy on the Transfer of Scientific, Technical and Engineering Information (NSDD-189) (September 1985, issued by Office of the President-Ronald Regan): Foundational federal document that outlined a national policy of openness in federally-funded fundamental research, including the fundamental research exclusion.

International Research Security Policies

G7: Canada, France, Germany, Italy, Japan, United Kingdom, and United States

1. G7 homepage
2. Best Practices for Secure and Open Research (February 2024)

Australia

1. Guidelines to Counter Foreign Interference in the Australian University Sector (November 2021): This provides guidelines for the Australian University sector to help manage and engage with risk to deepen resilience against foreign interference in the university sector.
2. China Defense Universities Tracker: A searchable database that provides ratings on "risk" for collaboration with an entity. In addition to the tracker, an associated document (released in 2019): Exploring the military and security links of China's universities

Canada

1. Safeguarding Your Research (October 2022): A government website that provides guidance and resources for researchers engaging in international research.

Denmark

1. Guidelines for international research and innovation cooperation (May 2022): Released from the Committee on guidelines for international research and innovation cooperation to facilitate international cooperation in research.

Japan

1. Policy Directions for Ensuring Research Integrity in Response to New Risks Associated with Increasing Internationalization and Openness of Research Activities (April 2021)

Sweden

1. Responsible internationalization: Guidelines for reflection on international academic collaboration (2020): Purpose is to aid universities in assessing collaborations and the best approach to international collaboration.

United Kingdom

1. Trusted Research (2019): A reference that can be utilized for advice and guidance which supports the integrity of the system of international research collaboration.