CHIPS Technology Protection Guidebook

A resource for implementing applicant and performer research security requirements

The CHIPS and Science Act provides $50 billion to the U.S. Department of Commerce (DOC) to strengthen and revitalize the U.S. position in semiconductor research, development, and manufacturing. CHIPS for America includes the CHIPS Program Office (CPO), responsible for semiconductor incentives, and the CHIPS Research and Development Office (CHIPS R&D), responsible for R&D programs, both within the DOC National Institute of Standards and Technology (NIST). CHIPS R&D will invest $11 billion to, among other goals, improve U.S. capacity to invent and deploy foundational semiconductor technologies, including for economic and national security purposes.

Unfortunately, competitor nations have aggressively sought to acquire U.S. intellectual property (IP) through licit and illicit means, including from academic and industry research organizations. Just as companies protect their intellectual property, ***CHIPS R&D must protect federally funded research products and the economic and national security advantages they provide***.

As a result, CHIPS R&D programs, including intramural and extramural research programs, will require applicants and research performers to implement research security measures. This document describes the CHIPS R&D research security approach and aims to provide applicants and performers with information to consider as they develop their own research security plans and programs. This guide is supplemental to any CHIPS R&D funding opportunity and for informational purposes only *(see disclaimer on page 7 for more information).*

Legislative Requirements and Context

Both Congress and the Executive Branch have sought to protect federally funded research and IP. Issued in January 2021, National Security Presidential Memorandum-33 (NSPM-33) aims to "strengthen protections of United States Government-supported R&D against foreign government interference and exploitation." NSPM-33 imposes disclosure requirements on federal funding recipients, seeks to standardize reporting requirements across agencies, and requires organizations that receive more than $50 million in annual federal R&D funding to implement their own research security programs. These research security programs must address cybersecurity, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. At the same time, Congress enacted into law[1] certain disclosure requirements, requiring "covered individuals" applying for federal R&D funds to disclose the amount, type, and source of all current and pending research support, including both monetary and non-monetary support.

Multiple Government and private-sector entities have issued documentation to support these research security requirements. In August 2023, NIST released NIST IR 8484 Safeguarding International Science Research Security Framework ("the Framework"), designed to help agencies and other interested

[1] Section 223 of Division A, Title II of the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 (FY21), (Pub. L. No 116–283, codified in 42 U.S.C. § 6605)

entities balance the traditional openness in the research community, research security, and international collaboration. The Framework outlines methodologies and requirements for an integrated, mission-focused, risk-balanced approach for safeguarding international science and technology from undue foreign interference while protecting the openness and integrity of the U.S. research ecosystem.

Addressing Research Security in CHIPS R&D Funding Applications

Leveraging the Framework, this guide seeks to provide potential applicants with best practices and high-level issues to address when including a research security plan or research security program in an application for CHIPS R&D funding. Notably, the guide focuses on research security considerations not limited to foreign collaborations.

CHIPS R&D recommends that a proposed research security plan or program discuss the following key elements, where applicable:

1. Establishing a Research Security Team and Methodology
2. Assessing At-risk Technologies and IP
3. Reviewing Personnel Appointments
4. Training Research Personnel and Staff
5. Reviewing Personnel Appointments
6. Reviewing Foreign Travel Requests
7. Reviewing Collaboration and Service Requests
8. Implementing Technology Control (e.g., Data Management and Export Controls)
9. Cybersecurity

Establishing a Research Security Team and Methodology

Effective research security begins with leadership commitment and establishing a team, which may include contracted staff, to develop and execute best practices and policies. Broad representation from across the organization can help ensure a shared understanding of both research security needs, promote acceptance of research security norms, and enable the incorporation of research security into other organizational objectives.

Applicants should consider identifying the following:

1. A research security Point of Contact (POC), including the POC name, position, and e-mail
2. Research security team members, including persons with expertise relevant to, if applicable:
    a. Scientific research
    b. Export control
    c. Information security
    d. Research and technology protection
    e. International engagement
    f. Cybersecurity
3. Additional *ad hoc* team members (e.g., legal counsel)
4. Specific roles and responsibilities for each team member
5. The expected scope of work (i.e., the reviews and assessments the team will conduct)
6. Organizational policies that define the research security team mission, methodologies for determining research security risks, and a process to adjudicate and approve relevant activities

Assessing At-risk Technologies and IP

CHIPS R&D has unique statutory requirements to ensure that federally funded IP remains subject to domestic control, to protect it from foreign adversaries. Consistent with this requirement and with other best practices, CHIPS R&D funding opportunities may ask proposers to identify pre-existing IP, IP that may be developed, and a plan for ensuring domestic control.

Applicants should consider identifying the following:

1. Any technologies or IP used or created during the research that may warrant protection from foreign adversaries, including technologies or IP resulting from fundamental research[2]
2. Processes to compartmentalize fundamental and non-fundamental research products and to enable pre-publication reviews of non-fundamental research products, if applicable
3. Concurrence with CHIPS R&D domestic control requirements and any required policies or procedures to ensure compliance
4. Any additional organizational strategies to protect intellectual property

Reviewing Personnel Appointments

It is NIST policy to create a culture of personal and organizational responsibility where the practice and management of research and its products are free from undue influence and interference not essential to the practice of science. Consistent with this policy and with NSPM-33, effective research security programs should identify and mitigate potential conflicts of interest or conflicts of commitment that could jeopardize scientific integrity or research products.

Applicants should consider identifying the following:

1. Processes for the organization to identify, and for personnel to report, organizational affiliations and commitments, including to meet the requirements of the Current and Pending Support Form
2. Processes for the organization to identify and address any potential conflicts of interest or conflicts of commitment, including malign foreign affiliations and funding

[2] For further information on identifying and protecting critical IP and technologies, consider reviewing the National Counterintelligence and Security Center Operations Security (OPSEC) Cycle.

Training Research Personnel and Staff

Communication and training ensure that employees and other research staff understand the need for research security protections, can identify research security risks and assess the benefits of collaboration, and consistently implement research security best practices. This training may include ongoing required training on broad topics and *ad hoc* instruction for specific situations or specific research programs, such as foreign travel, remote work, or export controls.

Applicants should consider identifying the following:

1. The scope, frequency, and source of any regular required training provided to research personnel and other staff, to include instruction on topics such as:
   a. Research integrity
   b. Research and technology protection
   c. Cybersecurity Identifying foreign talent recruitment programs
   d. Insider threat awareness and identification
   e. Securing research-related data
   f. Other responsibilities consistent with NSPM-33
2. The scope and source of any situational or program-specific training provided to research personnel and other staff
3. Any additional strategies for communicating research security incidents and concerns

Reviewing Foreign Travel Requests

NIST adheres to the principle that U.S. research leadership benefits from mutually beneficial international collaboration. However, to protect federally funded IP from foreign adversaries, CHIPS R&D statute prohibits funding a foreign entity of concern. Further, CHIPS R&D expects funded research to occur in the United States, absent NIST approval.

Applicants should consider identifying the following:

1. Internal processes for research personnel and staff to report foreign travel (including virtual conference/meeting attendance) if CHIPS R&D-related work will be conducted overseas
2. Procedures to evaluate the risks and benefits of work-related foreign travel, based on factors such as event type, purpose, and host organization
3. Processes to ensure that overseas travel does not provide a foreign entity of concern access to CHIPS-R&D funded research products
4. Provisions to provide research security briefings prior to foreign travel, to review data and device security measures and to, if necessary, remove project-related data from devices prior to travel
5. Provisions for personnel and staff, upon conclusion of foreign travel, to report any foreign adversary recruitment efforts or possible research compromises, if applicable

Reviewing Collaboration and Service Requests

CHIPS R&D encourages collaborative research between entities across the domestic semiconductor value chain, to include international collaboration, subject to NIST approval. Other entities may also seek access to CHIPS-funded tools, services, and information. In each case, the award recipient must adhere to research security requirements, including the protection of research conducted by their collaboration partners.

Applicants should consider identifying the following:

1. Processes for research personnel to report requests for collaboration or services (e.g., access to databases and tools), including foreign requests, and for notifying CHIPS R&D, as appropriate
2. Processes for evaluating the affiliations of prospective collaborators or service recipients, with criteria for approval
3. Processes to assess what technologies or IP, including technology or IP relevant to military applications, may be transferred as a result of the proposed partnership and for ensuring the application of appropriate export controls or other CHIPS R&D-specific protections, as relevant

Implementing Records Management, Cybersecurity, and Export Controls

Effective research security requires managing research documents and records. NIST, NSPM-33, and other federal Government policies and best practices often require activities to protect federally funded research data, including by addressing cybersecurity and export control concerns.

Applicants should consider identifying the following:

1. An up-to-date technology control plan, to protect against unauthorized transfer of IP and product groups
2. Compliance with the NIST Cybersecurity Framework

In addition to the above, applicants may describe, if applicable, a timeline to enhance any existing research security efforts and plans to inform CHIPS R&D of substantive changes (e.g., new personnel or collaborators). Applicants seeking additional information shall consult the Framework, which includes relevant checklists, or contact the NIST Research Security and Safeguarding International Science Team (researchsecurity@nist.gov).

GLOSSARY

Affiliations	Any past or present organization (foreign and domestic) with whom the associate has a formal relationship or obligation (e.g., universities, scholarships, professional societies, foreign talent recruitment programs).
Conflict of Interest	A personal interest or relationship that conflicts with the faithful performance of official duty. A situation in which an individual, or the individual's spouse or dependent children, has a significant financial interest, or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.[3]
Conflict of Commitment	A situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment.[4]
Covered Individual	An individual who (a) contributes in a substantive, meaningful way to the scientific development or execution of a research and development project proposed to be carried out with a research and development award from a federal research agency; and (b) is designated as a covered individual by the federal research agency concerned. NIST views authorship of a technical or scholarly publication as evidence of a truly substantial professional contribution, given an author's participation in conceiving or evolving the project design, executing significant aspects of the project, or documenting the project results in a form accessible to the scientific community.
Foreign Entity of Concern	Complete definitions of foreign entity of concern and foreign country of concern are found at 15 CFR part 231.
Foreign Talent Recruitment Program	An effort organized, managed, or funded by a foreign government, or a foreign government instrumentality or entity, to recruit science and technology professionals or students (regardless of citizenship or national origin, or whether having a full-time or part-time position).[5]
Fundamental Research	As established by National Security Decision Directive 189, 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.

[3] Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, January 2022.
[4] Ibid
[5] National Institute of Standards and Technology: Strengthening Disclosure Requirements and Assessing Training Could Improve Research Security, GAO-24-106074. A more specific definition is available via the OSTP Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs

Malign Foreign Talent Recruitment Program	A foreign government-sponsored talent recruitment program operated with the intent to import or otherwise acquire from abroad, sometimes through illicit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government.[6] A complete definition of malign foreign talent recruitment program is found at 42 U.S.C. 19237(4).
Research Security	Safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.
Technology Control Plan	A technology control plan assesses the project for export, transfer or disclosure controls on any data, equipment, or software and allowable access and ensures compliance with U.S. Government requirements (e.g., Export Administration Regulations, International Traffic in Arms Regulations).

Disclaimer

This guide is for informational purposes only and is intended solely to assist potential applicants in better understanding the CHIPS R&D application requirements. The guide does not, and is not intended to, supersede, modify, or otherwise alter applicable statutory or regulatory requirements or the specific requirements set forth in any CHIPS R&D Notice of Funding Opportunity (NOFO). In all cases, statutory and regulatory mandates, and the requirements set forth in the relevant NOFO, shall prevail over any inconsistencies contained in this guide.

Any reference to a non-federal organization or corporation does not convey endorsement or approval by the Department of Commerce of the entity or their programs or resources. All examples provided are for illustrative, non-exhaustive purposes only. The Department of Commerce does not guarantee the accuracy or completeness of the information contained therein.

[6] National Institute of Standards and Technology: Safeguarding International Science Research Security Framework, NIST IR 8484 (2023)