# Frequently Asked Questions: CHIPS R&D Research Security and Technology Protection

## Research Security Program and Research Security Plan Requirements

### 1. Why do the National Institute of Standards and Technology (NIST) and the CHIPS Research and Development Office (CHIPS R&D) care about research security and technology protection?

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.[1] In executing its responsibilities under the CHIPS Act and CHIPS and Science Act[2], CHIPS R&D must not only invest in research that improves U.S. economic competitiveness and the security of the domestic microelectronics supply chain but also protect that research from foreign competitors.

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

Congress and the Administration have taken several actions to guard federally funded research and IP. For instance, National Security Policy Memorandum 33 (NSPM-33) and its subsequent Implementation Guidance require certain Federal funding recipients to establish research security programs. In response, NIST's approach to research security seeks to balance the benefits of an open scientific research ecosystem and of international collaboration with the need to protect critical technology and IP.

### 2. What are the key elements of a research security program?

NSPM-33 requires that organizations receiving more than $50 million in federal R&D funding establish their own research security programs, which must address "cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training." Federal funding agencies may establish additional requirements for these programs, including to address risks to critical and emerging technologies such as semiconductors.

In August 2023, NIST published Safeguarding International Science: Research Security Framework (NIST IR 8484) to help provide guidance on establishing a successful research security program.

Several organizations have compiled additional guidance on addressing research security, including the National Counterintelligence and Security Center's collection of resources on Safeguarding Science, the National Science and Technology Council's Guidance for Implementing NSPM-33, the Association of American Universities' Science and Security Resource Document, and the National Science Foundation's research training modules.

To support applicants for financial assistance, CHIPS R&D plans to release further information on best practices, which include (but are not limited to) establishing procedures to:

- Provide research security training to relevant staff;
- Identify and mitigate conflicts of interest or conflicts of commitment;
- Mitigate foreign travel risks; and
- Review and approve foreign requests for research collaboration, products, or services.

## 3. Do entities applying for CHIPS R&D research funds need to demonstrate that they have a research security program in place before applying for a research award and/or before receiving research funding?

At present, CHIPS R&D does not require applicants to demonstrate the existence of a research security program in order to apply for or receive funding. However, applicants must provide a written plan (i.e., a research security plan) describing internal processes or procedures for addressing foreign talent recruitment programs, conflicts of commitment, conflicts of interest, research security training, and research integrity,3 as applicable.

## 4. Will CHIPS R&D require applicants that receive less than $50M in Federal R&D funds annually to have a research security plan?

Applicants for funding must respond to the requirements of the governing NOFO. All CHIPS R&D NOFOs will require a research security plan that demonstrates how the applicant will protect CHIPS R&D-funded research and associated data products from adversarial exfiltration.

## 5. Will CHIPS R&D require all subrecipients or subcontractors participating in a CHIPS R&D research to have their own research security programs or research security plans?

The award recipient is responsible for meeting NIST research security requirements, including the protection of all research conducted under the research award.

Some sub-awardees maybe subject to additional research security requirements. For instance, a sub-awardee that receives more than $50 million in Federal R&D annually would be subject to additional research security requirements under NSPM-33.

## 6. Will CHIPS R&D provide funding or other resources to establish or improve a research security program or to meet other CHIPS R&D research security requirements?

To date, CHIPS R&D has not established any specific programs or set-asides to support the development of a research security program. However, limited funding may be available to implement a research security plan, subject to the objectives of the individual notice of funding opportunity (NOFO) and the approval of the relevant program director. For entities selected to receive funding, NIST may provide assistance to establish or improve research security activities consistent with NIST best practices (NIST IR 8484).

## 7. How and when will NIST assess the adequacy of a research security program or research security plan?

During the review of the application, the NIST Research Security and Safeguarding International Science Team will use NIST IR 8484 as the basis for reviewing and assessing research security risks. In conducting its assessment, NIST will consider factors such as the type of research to be conducted (e.g., fundamental vs. proprietary research), potential dual use applications (e.g., military and civilian), and the benefits of the research collaboration. NIST will also review available information (e.g., the Current and Pending Support Forms and Resumes or CVs) to assess whether the applicant or any covered individuals are subject to any undue foreign influence or interference by foreign strategic competitors or governments of countries that have a history of IP theft, research misconduct, or targeting U.S. technology for unauthorized transfer. If the NIST Research Security and Safeguarding International Science Team issues a risk determination that an application presents a high risk, NIST may provide the applicant, at its sole discretion, an opportunity to mitigate the assessed risk prior to CHIPS R&D making a final funding determination on the application. This research security assessment will occur separate from the CHIPS R&D evaluation based on the evaluation criteria defined within the funding opportunity.

## Foreign Entities of Concern

### 1. What is a foreign entity of concern?

To protect national security and the resiliency of supply chains, CHIPS for America funds may not be provided to a foreign entity of concern, such as an entity that is owned by, controlled by, or subject to the jurisdiction or direction of the governments of China, Russia, North Korea, or Iran.

Complete definitions of foreign entity of concern and foreign country of concern are found at 15 CFR part 231.

### 2. Can persons from a foreign country of concern participate in research?

In general, restrictions on foreign entities of concern would not alone prevent an individual lawfully present in the United States from participating in CHIPS R&D-funded research. However, such individuals are subject to an individualized research security assessment. Prospective applicants and subcontractors are encouraged to contact the NIST Research Security and Safeguarding International Science Team (researchsecurity@nist.gov) for guidance on specific potential scenarios.

## Fundamental Research

### 1. What is fundamental research?

As established by National Security Decision Directive (NSDD) 189:

*'Fundamental research' means 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.*

### 2. Will CHIPS R&D NOFOs support fundamental research, proprietary/restricted research, or a combination of both?

Applicants for funding must respond to the requirements of the governing CHIPS R&D NOFO, which may include support for fundamental research, proprietary/restricted (non-fundamental) research, or a combination of both.

CHIPS R&D funding opportunities may ask an applicant to indicate, in their proposals, whether the applicant considers all or part of their work to be fundamental or proprietary. In instances where multiple types of research are contemplated, the applicant must describe their intent to compartmentalize fundamental and non-fundamental research activities and products. NIST and CHIPS R&D, however, reserve sole discretion to determine which elements of a proposed research project shall be considered fundamental or proprietary research. Wherever feasible, NIST and CHIPS R&D will seek to consider basic or applied research conducted on campus at a university as fundamental research.

### 3. Can an organization publish CHIPS R&D funded work with a foreign entity of concern?

Foreign entities of concern cannot be recipients of CHIPS funds. Publication with a foreign entity of concern shall be subject to a pre-publication review and approval by the CHIPS R&D Program Office.

### 4. Can an organization assume that its research products are not subject to U.S. export control laws, because the organization intends to publish its research results or because NIST or CHIPS R&D has identified the research as fundamental?

No. Although fundamental research is not generally restricted by Export Administration Regulations (EAR), applicants are responsible for ensuring compliance with all export control limitations.

## Research Participants and Covered Individuals

### 1. How will the CHIPS R&D program define “covered individuals”?

The definition of a “covered individual” only applies to extramural research funded by NIST. The CHIPS and Science Act defines a “covered individual” as 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.

Those designated as covered individuals must disclose the amount, type and source of all current and pending research support, which includes both monetary and non-monetary support, and certify that the disclosure is current, accurate, and complete. All covered individuals will undergo a NIST research security review that includes consideration of, for instance, current and pending research support and potential conflicts of interest or conflicts of commitment.

NIST generally does not consider individuals who only conduct isolated tasks incidental to the research (for example, setting up equipment or performing administrative functions) or individuals who support research by executing discrete tasks as directed as covered individuals. Consistent with guidance for implementing NSPM-33, disclosures from broader classes of individuals (e.g., certain graduate students and undergraduate students) will generally be unnecessary, except when the activities of such an individual in a specific proposal rise to the level of meeting the definition of a “covered individual” under 42 U.S.C. § 6605(d)(1). For instance, NIST views authorship of a technical or scholarly publication as evidence of a truly substantial professional contribution to the research, given an author’s participation in conceiving or evolving the project design, executing one or more significant aspects of the project, or documenting the project results in a form accessible to the scientific community.

2. When in the funding process (proposal, review, negotiation, award) will CHIPS R&D require applicants to identify covered individuals?

   CHIPS R&D funding opportunities will require that applicants identify “covered individuals” as part of their application. Successful applicants must update the list of covered individuals as additional personnel are hired or onboarded, in accordance with the NOFO.

3. Can foreign citizens participate as covered individuals and work on a CHIPS R&D-funded research project?

   Subject to a research security review, foreign citizens who are designated as covered individuals may participate in CHIPS R&D-funded research as long as they do not fall within the definition of a “foreign entity of concern.”

## International Travel

1. Are project participants subject to additional disclosure and monitoring with regard to international travel?

   All award recipients will be required to provide training to individuals participating in the funded research. This training shall include guidelines for protecting project information during personal and professional travel. Travel to a country of concern shall be subject to additional review.

2. Can individuals work remotely outside the United States on CHIPS R&D-funded research?

   Remote work will be addressed in the operational security element of the Awardee’s research security plan. In general, research security programs endeavor to enable flexibility for individuals while protecting research information and program data. To the extent that remote work is expected to be necessary, CHIPS R&D will work with Awardees to ensure the protection of project data. Remote work in a foreign country of concern is not allowed. Prospective applicants should contact researchsecurity@nist.gov to discuss any specific scenarios they anticipate having to address.