**NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314**

NSF 23-123

Dear Colleague Letter: Workshop to Inform Development of the NSF Research on Research Security Program (RRSP)

June 29, 2023

Dear Colleagues:

Since World War II, the U.S. has been a global leader in science and technology (S&T) research and innovation. The U.S. S&T research model—and that of like-minded allies and partners—emphasizes benefits that accrue to all in an open, transparent research ecosystem. This is possible because most participants share a commitment to the fundamental principles and values essential to the conduct of research. Unfortunately, these principles and values are not shared by some foreign governments which choose to interfere with or inappropriately benefit from U.S. S&T research. These governments do so by using a systems-wide approach to obtain pre-publication data and results, methods and knowhow, intellectual property, and talent. Such violations threaten the security of the U.S. S&T research ecosystem.

To more fully understand the nature, scope, challenges, and potential of research security across all research, particularly in the context of National Security Presidential Memorandum-33 (NSPM-33) and associated supporting documents, NSF is developing a new Research on Research Security Program (RRSP). With this Dear Colleague Letter (DCL), NSF is seeking proposals for a workshop[1] that will bring together researchers who conduct or have an interest in conducting research in this domain, with the intent of raising awareness of the RRSP and developing a community of practice that includes institutions of higher education, for-profit organizations, governmental entities, and non-profit organizations to conduct this highly interdisciplinary research.

OBJECTIVE

With this DCL, NSF seeks proposals to organize and facilitate a single workshop that will bring together diverse perspectives and stakeholders from all sectors of the research community, particularly those already engaged in research security-related research, to identify:

A. Themes and topics that should be studied in the RRSP (see Potential Themes/Topics);
B. Special considerations for and/or barriers to conducting research on the themes and topics, especially access to relevant data and associated statutory or regulatory restrictions; and
C. Approaches that might be used to study the themes and topics systematically, qualitatively, and/or quantitatively.

These discussions will help build new and strengthen existing relationships that will lead to the collaborations necessary for the RRSP to be successful. Findings from the conference will be shared publicly in the form of an open-source report or other comparable communication mechanisms.

POTENTIAL THEMES/TOPICS FOR PROPOSALS

NSF has included in this DCL a non-comprehensive list of potential RRSP themes/topics to serve as a starting point for conference proposals. Themes/topics may be added or modified as deemed appropriate and need not be mutually exclusive. Themes/topics form the foundation for addressing Objectives B (barriers) & C (approaches). Identifying barriers that, if removed, would provide the greatest opportunity for the research on research security community would be especially valuable. As appropriate, this work should consider variability based on researcher career stage & identity; fields of research; research motivation (foundational, curiosity-driven, use-inspired, applied, translational); sectors of the research enterprise (industry, government, academia, non-profit organizations); technologies; organizational types; and nations.

Nature and Pervasiveness of Research Security Threats

1. The type, prevalence, frequency, seriousness, and potential implications and impacts of research security threats and violations, and the fields and technologies targeted most often.
2. Factors that motivate or compel individuals to violate research security rules and regulations.
3. Factors that justify classification or other restrictions on open basic/fundamental research.
4. Threats to the basic/fundamental research ecosystem that might result from overly aggressive or insufficiently aggressive approaches to addressing research security issues.
5. Real or perceived constraints on academic freedom resulting from research security rules and regulations.
6. Contrasts in research security risks between use-inspired and curiosity-driven foundational research[2], as well as research security risks across the spectrum from

foundational, applied, and translational research.
7. The ability to predict research security threats and violations, the data needed to make such predictions, and quantification of uncertainty associated with predictions.

Research Security Threat/Violation Identification, Mitigation and Prevention

1. The extent to which researchers and research organization leaders understand research security threats and current efforts to address them and the sources of information that have informed their understanding.
2. The effectiveness of current education and training efforts in research security and ways in which such effectiveness can be improved.
3. The impact on identification, mitigation, and prevention of research security threats and violations resulting from differing opinions and disinformation about science and research.
4. Factors that discourage individual and institutional reporting of research security threats and violations, and actions that can be taken to improve reporting.
5. Use of quantitative risk measurement and mitigation capabilities for research security threat and violation detection and prevention.
6. Use of artificial intelligence (AI) to help identify and mitigate research security threats and violations and ways in which AI might unintentionally or intentionally enhance them.

International Dimensions of Research Security

1. A comparison of U.S. actions in research security with those of other nations, the possibility and desirability of international collaboration in research security, and criteria for guiding the selection of partner nations with which the U.S. should collaborate on research security.
2. Impacts from research security threats and domestic policy decisions on recruitment and retention of foreign STEM talent, including factors and information sources that influence foreign nationals' decisions to study or conduct research in the U.S. or elsewhere.
3. Impacts of real and perceived stigmatization on research security threat identification and mitigation, and strategies for overcoming them.

PARTICIPANTS & FORMAT

The workshop should engage a diverse array of national and international experts, from an equally diverse array of public and private organizations, in the following domains: social, behavioral, and economic sciences; physical, natural and life sciences; mathematical sciences; engineering, computer science, data science & cybersecurity; international relations; and law enforcement and intelligence. NSF supports Broadening Participation efforts by soliciting and encouraging proposals from the full spectrum of diverse talent that society has to offer. Workshops may be virtual or in-person or contain elements of both. However, to maximize participation at in-person workshops, NSF encourages a virtual option for those who cannot or wish not to travel.

TIMELINE

Proposals submitted in response to this DCL will be accepted until September 25, 2023 (5 p.m. submitter's local time). The award is expected to be made by December 2023, with conference findings synthesized by June 2024.

PROPOSAL PREPARATION INSTRUCTIONS

Proposals must be prepared following the guidance for conference proposals contained in Proposal & Award Policies & Procedures Guide (PAPPG) Chapter II.F.9. In addition, proposals must describe (a) how workshop participants will be selected and supported and (b) how input will be collected and synthesized. Proposals should include a plan and timeline for sharing the conference findings to ensure broad communication across all sectors of the research community.

Proposals submitted in response to this DCL must include the prefix "RRSP" in front of the title. If using Research.gov, the system will automatically insert the prepended title "Conference" and that should be followed by "RRSP:". Proposers should select the current PAPPG as the funding opportunity and direct proposals to the Research on Research Security Program (RRSP) in the Office of Integrative Activities (OIA) in the Office of the Director (OD).

Proposal budgets must be well-justified for the scope of the proposed activities and participants. Budgets may be up to $75,000 total, inclusive of facilities and administrative costs. Funds may be included to support staff who will facilitate conference discussions and prepare the final report.

The "Research Security at the National Science Foundation" website (https://new.nsf.gov/research-security) contains a collection of definitions, tools, reports, and policies that are relevant to this DCL. Reports include recommendations on research security challenges and best practices from other nations. Involving experts from like-minded nations in this conference is strongly encouraged.

WEBINARS

NSF will hold informational webinars regarding this DCL on Thursday July 13, 2023 at 4 p.m. EST and Wednesday July 26, 2023 at 2 p.m. EST. Register for either identical webinar here. Webinars will be recorded and posted on the NSF Research Security website.

Inquiries about this DCL and questions about submission of proposals should be directed to RRSP@nsf.gov.

Sincerely,

Rebecca Keiser
Chief of Research Security Strategy and Policy

REFERENCES

[1] Also referred to as conferences in Proposal and Award Policies and Procedures Guide (PAPPG) Chapter II.F.9.

[2] Stokes, Donald E. Pasteur's Quadrant. Washington, D.C., Brookings Institution Press, 1997.