COGR

June 27, 2023

Submitted by Email to: RSI-ISAO@nsf.gov
Rebecca S. Keiser, Ph.D.
Chief of Research Security Strategy & Policy
Office of the Director, National Science Foundation (NSF)
2414 Eisenhower Ave.
Alexandria, VA 22314

RE: Comments in Response to Dear Colleague Letter: Development of the U.S. Research Security and Integrity Information Sharing Analysis Organization

Dear Dr. Keiser:

COGR is an association of over 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. We focus on the impact of federal regulations, policies, and practices on the performance of research conducted at our member institutions, and we advocate for sound, efficient, and effective regulation that safeguards research and minimizes administrative and cost burdens. COGR and its member institutions recognize the importance of ensuring research integrity and responding to malign foreign influence on federally funded research. Our institutions have worked at considerable time and cost to develop and promote effective practices in this area, while fostering international collaborations that are vital to the success of the U.S. and global scientific enterprise.

We thank NSF for holding a robust listening session on June 7, 2023, with representatives from COGR member institutions and staff to discuss the proposed Research Security and Integrity Information Sharing Analysis Organization (RSI-ISAO). We deeply appreciate NSF's willingness to engage in open and frank discussions with the academic research community on the RSI-ISAO's proposed structure and duties, and we are following up with additional comments in response to the May 4, 2023, Dear Colleague Letter.

First and foremost, COGR fully supports the development of the RSI-ISAO. We believe strongly that the key to the organization's success is ensuring that it is structured and operated in a manner designed to engender community trust. We were pleased that during the June 7 listening session NSF set forth the following expectations for the RSI-ISAO:

- The RSI-ISAO will serve as a neutral, non-governmental venue in which institutions may choose to participate;
- The RSI-ISAO will not have an enforcement role and will not act as an intermediary in reporting information from institutions to enforcement agencies; and

- The RSI-ISAO will be transparent about its role and operations, and well as the type of information it will receive and how it uses that information.

Achieving these objectives is essential to ensuring that the RSI-ISAO has an operational framework designed to foster the trust and participation of academic research institutions. We further urge NSF to make certain that the RSI-ISAO's charter explicitly: (a) recognizes the need for institutions to employ **risk-based assessment and mitigation strategies** when analyzing research security issues; and (b) calls for the development and provision of clear, easy-to-use tools and specific threat information that institutions can utilize in their analyses.

Below are additional comments that respond to thematic areas 1, 2, and 7, as described in the Dear Colleague Letter. These comments are based on discussions with, and a pre-listening session survey of, a representative sample of COGR member institutions.

Thematic Area 1, Current Security and Integrity Issues – What types of research security and integrity issues do you encounter on a day-to-day basis?

One of the most common research security-related questions that institutions receive from faculty members is: "*Can I carry out this fundamental research activity with collaborators or an institution located in China, or will doing so put my federal funding in jeopardy*?" This question frequently arises in the context of evaluating standard, academic relationships (e.g., sabbaticals, collaborative research) that do not bear hallmarks of illicit activity, such as dual full-time employment or inappropriate transfer of intellectual property, but may include research activities in China. Although NSF and other federal agencies consistently voice support for international collaborations, to date federal research security guidance does not explicitly endorse the concept of risk-based assessments,[1] nor does it include any affirmative guidance for if and how collaborations with China can be appropriately conducted.

Clear guidance from the RSI-ISAO on these topics is essential to helping institutions navigate the security landscape. **Further, RSI-ISAO tools must account for the fact that not all countries present the same security risk,** and they must identify those countries, institutions, and individuals with higher risk profiles. Applying the same standards to all "foreign" collaborations and collaborators would do nothing to promote equity in terms of actual risks presented. Rather, it would impose "high-risk" requirements on collaborative research conducted with "low/no risk" foreign institutions. This approach would result in unwarranted impediments that would harm, if not crush, important research efforts with institutions in countries whose research integrity values and practices align with those of the U.S.

Thematic Area 2, Informational Resources -- Based on the duties for the RSI-ISAO specified in the CHIPS and Science Act of 2022 and listed above, what resources should the RSI-ISAO provide to the research community to inform decision-making, management, and mitigation of research security and integrity risks?

The RSI-ISAO should provide up-to-date, credibly sourced, clear, specific, actionable information concerning high-risk actors, institutions, countries, entities, and programs. In particular, institutions should

[1] *See,* COGR, Response to Request for Information; NSPM 333 Research Security Programs Standard Requirement (May 30, 2023).

be provided with ready access to all updated “lists” of identified high-risk individuals and entities that they are charged with reviewing. We acknowledge that such entities may take actions (e.g., name changes) to evade these lists, but that fact lends further support for a robust RSI-ISAO that provides institutions with access to the most up-to-date threat data, as opposed to denying institutions access to this critical information.

In addition to information, the RSI-ISAO should equip institutions with tools that they can use in analyzing research security issues. Such tools include risk assessment matrices, case studies (including studies of successful international collaborations), mitigation plans/techniques, decision trees, and flow-charts.

Finally, the RSI-ISAO should establish a “safe-space” forum that facilitates open, two-way communication between the RSI-ISAO and its members without fear of penalty or reprisal.

Thematic Area 7, (Optional) Additional Feedback

In addition to our prior comments concerning the listening session, we also wish to commend NSF for recognizing that transitioning the RSI-ISAO from a fully government-supported to an institutional fee-based, membership model may significantly harm the ability of institutions to participate, particularly smaller and emerging research institutions. Although institutions in our pre-listening session survey ranked the utility of guidance and resources provided as the factor with the greatest impact on their decision to participate in the RSI-ISAO, several institutions commented on how membership costs may discourage participation, and thus limit the RSI-ISAO’s reach and utility.

Conclusion

COGR members take seriously research security threats and their responsibility to help, identify, deter, assess, and address them. The RSI-ISAO has the potential to be a significant new resource for institutions in assessing the research security landscape, but only if it is structured in a manner that ensures both its trustworthiness and utility. We believe our recommendations serve both those goals, and we appreciate NSF’s consideration of them.

Finally, we wish to note the comments that EDUCAUSE submitted in response to the Dear Colleague Letter regarding the role that the RSI-ISAO may play with respect to cybersecurity issues. We support its recommendation that the RSI-ISAO leverage and extend the information and sharing analysis functions of established, relevant information sharing and analysis centers while avoiding the duplication or fragmentation of current threat sharing mechanisms. We also support EDUCAUSE’s comments regarding the cybersecurity information resources that the RSI-ISAO can provide and the prioritization of the RSI-ISAO’s duties in the cybersecurity sector.

Should you have any questions concerning this response, please feel free to contact Kristin West, Director, Research Compliance and Ethics or Robert Hardy, Direct, Research Security and Intellectual Property.

Sincerely,

M.M.Owens

Matt Owens
President