Association of American Universities
America's Leading Research Universities

**MEMORANDUM**

TO: RSI-ISAO@nsf.gov

FROM: Association of American Universities
Tobin Smith, toby_smith@aau.edu
Meredith Asbury, meredith.asbury@aau.edu

DATE: June 30, 2023

Re: Request for Input on the Development of the U.S. Research Security and Integrity Information Sharing Analysis Organization; NSF 23-098

On behalf of the Association of American Universities, which represents America's leading research universities, we appreciate the opportunity to provide input in response to the "Dear Colleague" Letter issued by NSF on May 4, 2023 regarding the development of the U.S. Research Security and Integrity Information Sharing Analysis Organization.

Universities take seriously the threats posed by malign foreign actors. In recent years, as our members have become more aware of the threats to university-based research posed by malign foreign actors, AAU institutions and their faculty have stepped up efforts to protect the integrity of federally funded research. We therefore welcome a risk-assessment center that will help support the research community's efforts to address risks while continuing to encourage and support the international scientific research collaboration necessary for scientific advancement and innovation.

**Informational Resources**

One of the primary goals of the center should be to provide the research community with actionable information that can be used to inform an institution's decision-making and enhance their efforts to assess and mitigate risks posed by foreign entities. For the center to be effective, information on research security risks and threats must be timely, usable, and digestible by many types of institutions. Information could be useful in several forms including alerts, an information-sharing community, webinars, and reports. In particular, any analysis drawn from information that is publicly available should also remain publicly available and unclassified. Too often information collected by federal research security agencies from open-source materials is classified and therefore inaccessible to institutions to help inform their assessment of risks. The center will be well positioned to provide information as a publicly available, unclassified resource.

In addition, we support the center providing analysis that bridges an existing gap between publicly available information and agency guidelines. As part of the center's 'clearinghouse' duties, it could collect publicly available agency practices and provide analysis that helps to align risks with concerns of agencies. This can be done in a non-binding way.

As much as possible, the center should create opportunities to engage with university officials directly using webinars, awareness and information-sharing sessions, and trainings. The center should continually analyze the use of informational resources and adapt resources based on community feedback. The center should also maintain information that helps address threats to all federally supported research and not be limited to NSF-sponsored research activities.

**Liaison Role**

One of the key roles of the center should be to convene non-government and government stakeholders to allow for broad-based information sharing on key research security and integrity issues. One critical function the center should provide is to serve as an information-sharing hub for the universities that it serves. As universities become more sophisticated in their efforts to identify and mitigate research security risks, it will be increasingly important for institutions to share what they have learned with each other. In addition to providing a forum for universities to share information among themselves, the center will also be well-positioned to connect research institutions with government agencies for the purpose of sharing information and developing stronger working relationships to support research security. In fulfilling this liaison role, the center's convenings may also eliminate the need for duplicate forums or meetings where federal research and security agencies convene and discuss research security with smaller subsets of institutions.

**Equity and Sustainability**

The DCL does not currently address how the center will be funded and sustained in future years of work. The existing ISACs and ISAOs for cybersecurity created by the Department of Homeland Security have often operated as a member organization, with set fees to participate and receive access to information. If a similar funding model is adopted for this organization, it will complicate information-sharing particularly for smaller, less resourced institutions; that would ultimately harm the effectiveness of the center.

NSPM-33 states that institutions which receive $50 million or more in federal research funding in a year must establish a research security program. However, even institutions that receive less research funding may benefit from having access to the timely analysis and information which this center will be able to provide. We hope that the center will provide equitable access to all institutions required to maintain a research security program. We understand that NSF will provide support for the center to ensure it is stood up and accessible. We would encourage that a long-term, non-dues-dependent model be adopted so that all U.S. institutions that can benefit from the center's information and analysis services.

**Conclusion**

We look forward to continuing to engage with NSF as the risk assessment center is developed. Should you have any questions, please contact us using the information provided above.