

Cornell University

Office of the Vice President
for Research and Innovation

Krystyn J. Van Vliet

222 Day Hall

Ithaca, New York 14853-2801

t. 607.255.7200

f. 607.255.9030

krystyn.vv@cornell.edu

June 30, 2023

Rebecca S. Keiser, PhD
Chief of Research Security Strategy and Policy
Office of the Director
National Science Foundation

Cornell University White Paper Responding to NSF 23-098 Dear Colleague Letter: A Request for Input on the Development of the U.S. Research Security and Integrity Information Sharing Analysis Organization (RSI-ISAO)

Cornell University, a leading U.S. institution of higher education and academic research, welcomed the passage of the CHIPS and Science Act of 2022 (the Act). Cornell is eager to increase our participation in the broad range of important fields of research, education, and U.S. workforce development that it funds. Cornell appreciates and supports the concurrent goal of national security through strengthening the United States' position as a global leader in semiconductor research, development, and manufacturing – including but not limited to adherence to existing U.S. regulations and guidance including export control considerations. As a university, Cornell is also dedicated to open, transparent, and inclusive education of and research conducted by U.S. citizens and those from other countries that the U.S. government has approved to study in or work in the U.S. At present, Cornell and similar U.S. research universities have identified challenges to interpreting the requirements of National Security Presidential Memorandum 33 (NSPM-33) in a manner that allows us to properly prepare to comply with upcoming research security program requirements while meeting our obligation to perform basic and fundamental research in the open manner that best ensures its integrity and impact. Achieving this balance is a challenge shared by all U.S. research universities, and we are pleased to aid the effort by adding our reply to the NSF 23-098 Dear Colleague Letter.

Cornell welcomes the establishment of the RSI-ISAO as a source of information. Cornell also supports and participates in the efforts of college and university associations including the Council on Government Relations (COGR) to better define research security program requirements. The following paragraphs comprise Cornell's input on the six thematic areas described in the Dear Colleague Letter.

1. Current Research Security and Integrity Issues:

Universities are structured as locations of organized and investigator-initiated research. Academic freedom regarding topics of research inquiry, methods of inquiry, is critical to the quality and quantity of research results that make Cornell a world class institution. With that freedom of the university research investigator comes the responsibility for the integrity of reported research results and, as appropriate to the research, for acceptable practices of research related to safety of the researchers and wider community. That responsibility is shared by the research leader – a university employee often called the principal investigator or PI in federally sponsored research projects – and the university administration – as one important channel to provide information, training, and appropriate oversight of external requirements on the PI's research). Consequently, Cornell's principal research security and integrity activities focus on keeping researchers informed of changing regulatory requirements that apply to their discipline, monitoring their specific activities well enough to provide necessary guidance, and accomplishing these tasks without burdening them to the detriment of their research progressing toward positive societal impact.

The Cornell research community recognizes that all research data need to be protected from corruption or theft by cyberattack or other malign actions. Such protection is reasonably well accomplished by: (1) cybersecurity protection practices of university-managed information technology (IT) systems; and (2) university policy that asserts Cornell ownership of research data and that requires administrative access to that data, thus ensuring storage on university-owned equipment including research instrumentation and research computing resources. However, the university community is much broader than the research community, and it is acceptable practice for students, staff and faculty to use personal devices such as phones and computers for Cornell related activities while also following Cornell policies related to research data security. Extension of the expectation focused on research data

security to include personal devices and software that are not used for research primarily or exclusively represents a large and unsupported cost that would be prohibitive to implement. Importantly, such a broad approach to cybersecurity of devices would not present a clear improvement on risk mitigation over current cybersecurity protection practices of university managed IT systems and research data access policies and practices.

The Cornell research community also recognizes that the unauthorized sharing of data, particularly with bad actors, may be harmful to research sponsors or national security. However, sharing data and knowledge with the broader research community is critical to the integrity and viability of fundamental research and education, and to maintaining excellence of the U.S. research community on and beyond university campuses. Guidance to help individual researchers achieve this delicate balance requires clear and specific statements of what actions are not allowed by the government, in contrast to sharing risk awareness and mitigation options. General statements regarding activities that might be of concern are not particularly helpful. General and vague statements can lead to misunderstanding and noncompliance, or worse, unintentionally debilitating restrictions by organizations trying to ensure compliance.

2. Informational Resources:

The most important information the RSI-ISAO can provide to the research community is clear and specific identification of bad actors and organizations that are to be avoided. Vague, or ambivalent statements create unnecessary anxiety and fuel discriminatory behavior against researchers. For example, simply stating China is a foreign entity of concern creates anxiety for individuals of Chinese citizenship or family origin and creates the working environment, if not the fact, of discrimination against researchers legitimately working and studying in the United States.

As in other universities, the research community at Cornell comprises thousands of individuals. Correctly applying ambiguous information to each individual situation is not practical and can be impossible. Timely alerts on current concerns are helpful if they are clear and specific, but alerts that are general or ambiguous are more problematic than useful.

Specific, actionable, guidelines that embrace open fundamental research are needed. Webinars and other meeting formats that encourage communication between the RSI-ISAO and the research community will help ensure that guidelines are useful and not harmful to the research enterprise.

3. Prioritization of the RSI-ISAO's Duties:

Our ranking of the seven duties required by the CHIPS act, briefly stated, is as follows:

1. Provide training and support, including through webinars, for relevant faculty and staff;
2. Serve as a clearinghouse for information;
3. Share information concerning security threats and lessons learned;
4. Develop a standard set of frameworks and best practices;
5. Enable standardized information gathering and data compilation, storage, and analysis;
6. Provide timely reports on research security risks to provide situational awareness;
7. Support analysis of patterns of risk and identification of bad actors.

4. Integration:

A standard set of frameworks and best practices provided by the RSI-ISAO will be very helpful to simplify development and maintenance of related compliance policies and programs. To integrate these resources into our research security and integrity decision-making process, we will designate a Cornell compliance or data security officer as our research security point of contact. This person and RSI-ISAO frameworks will be particularly important in establishing a robust method of providing research security enclaves tailored to the needs of sponsor contracts. We expect this will be critical to efficiently protect research data that requires more than the basic cybersecurity protecting all Cornell infrastructure.

Training and support for relevant faculty and staff would be very helpful. Staff responsible for compliance programs meeting the requirements of the Act of 2022 will benefit from webinars and interactive training with RSI-ISAO staff to ensure Cornell programs fully meet the requirements of the act. Individual researchers will benefit from training videos as reminders of their responsibilities under the compliance programs. Researchers will be best served if the videos are brief (10 minutes or shorter), concise, and interactive (e.g., video followed by short question/answer). Websites conveniently locating relevant training information will be helpful for staff and researchers. We strongly support aligned research security requirements across all agencies, including but not limited to the requirements under the Act, and national security presidential memorandum 33 (NSPM-33). To the

extent that is not feasible, clear visual charts noting any special requirements of specific agencies would be most helpful.

Cornell envisions using the information clearinghouse in two primary ways. First, it will help us continuously review and update our data security enclave methods. Second, specific information on bad actors and programs to avoid will be used to continuously update our Conflict of Interest (COI) and Export Control programs. Many universities rely on the [Australian Strategic Policy Institute's risk tracker](#) as a tool for assessing program risk. A similar tool more closely aligned with the intentions of the Act could be easily integrated into university COI and Export Control programs and would be very helpful.

Clearinghouse information would be most efficiently distributed by a listserv, or similar electronic distribution method, for compliance and security personnel. Email announcements and explanatory webinars would help personnel make effective use of new information.

5. Benefits based on Position:

RSI-ISAO resources will principally benefit staff and executive officers responsible for developing compliance and security policy and procedures. Staff responsible for monitoring research activities and assisting researchers in regulatory compliance will also benefit, but to a lesser extent than those responsible for policy and procedures. Direct benefit to other members of the Cornell community is limited due to reliance on compliance and security staff who monitor and interpret federal regulation. Researchers will primarily benefit from effective compliance programs and training that they receive from staff, who will be well informed by RSI-ISAO resources.

A timely and well-curated clearinghouse of information related to risk, a standard set of frameworks and best practices for risk mitigation, and training suitable for researchers will help reduce the work staff need to do to monitor potential conflicts of interest and research data security weaknesses. However, effective and efficient research security requires that the frameworks, best practices, and guidance are in common or at least not contradictory among all federal agencies. Reducing this work at universities associated with understanding and deconflicting information of different U.S. agencies, policies, research sponsor requirements, and memoranda will reduce the likelihood that researchers will inadvertently be non-compliant.

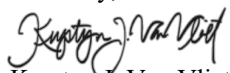
The cost of ensuring research security is always important, and more so to those institutions with more limited resources beyond those provided by research sponsors. Most U.S. university research is sponsored by the federal government, and does not anticipate additional costs associated with research administration for which reimbursement by the government is capped. It is not clear to us that sustaining the RSI-ISAO through membership fees is an appropriate way to utilize the resources of all the institutions that need this service. To encourage usage that will benefit both this new organization and the U.S. research security and integrity goals of the Act, a model that considers this a government-funded resource rather than a subscription user model is recommended strongly.

6. Liaison Role:

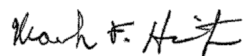
The RSI-ISAO can play a useful role as a liaison among research institutions by identifying and reporting concerns and trends that appear common across the institutions. We believe it is crucial that the RSI-ISAO have a board of directors and that board include representatives of the Higher Education Community to enhance understanding and trust.

A mechanism to answer confidential questions privately would improve understanding and enhance trust. Federal agencies benefit from better understanding of university operations, especially the differences from for-profit corporations or federally funded research organizations that conduct classified research. Likewise, universities need to understand the government's concerns through specific shareable information and prior case studies, even when the seriousness of the concern is appreciated and shared. The RSI-ISAO can play a strong role in promoting that understanding by acting as a trusted partner and forthrightly elevating common issues to the agencies. This will do much to create better understanding between the federal government and the U.S. academic research community.

Sincerely,



Krystyn J. Van Vliet
Vice President for Research and Innovation



Mark Hurwitz
Chief Research Compliance Officer