Responsible Conduct of Research (RCR) Research Security Training

The CHIPS and Science Act of 2022 (Section 10337) directs the National Science Foundation (NSF) to require several additions to Responsible Conduct of Research (RCR) training while also expanding the training to faculty and other senior personnel. The additions include “training to raise awareness of potential research security threats; and Federal export control, disclosure, and reporting requirements.” This module outlines the role of research security in RCR in compliance with the CHIPS Act and NSF requirements. It has been adapted from the NSF SECURE Center research security condensed training module. Information for Senior/Key Personnel is abbreviated as the topics are addressed in depth in the research security training NSF and other agencies require Senior/Key Personnel to take prior to proposal submission consistent with the CHIPS Act.

Select your Role

Senior/Key Personnel Supported on an NSF Award(s)

LAUNCH MODULE

Non-Senior/Non-Key Personnel Supported on an NSF Award(s)

Select this option if you are not senior/key personnel on an NSF award. If you were designated senior/key personnel on an NSF award (e.g., Principal Investigator (PI), Co-PI, or other senior) you would have submitted biosketch and current and pending support forms.

LAUNCH MODULE

Research Security for Senior/Key Personnel

Research Security Overview

Research security is about safeguarding the research enterprise against the misappropriation of pre-published or pre-patented research and development (R&D) to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

Research security includes components, such as 1) adherence to regulations, policies, and procedures, 2) protection against intellectual property (IP) theft, misuse, and sharing of, or unauthorized access to, pre-published or pre-patented information, and 3) mitigation of research security risks. Research security also includes ethical research practices, such as disclosure of research-related relationships, financial interests, and transparency of foreign activities and collaborators.

Disclosure and Reporting

Accurate and timely disclosure of outside activities and research support will support ongoing research security efforts. In general, researchers need to disclose all research-related activities, academic, professional, or institutional appointments and positions, and sources of support for any of their research endeavors, regardless of whether they are through a researcher's home institution or directly to the individual, or whether they have monetary value. Please ensure that you are familiar with each agency's disclosure requirements prior to applying for funding as well as those of the University. You can find information on disclosure on your university's website [Add Hyperlink to University Disclosure Page].

Potential Research Security Risks & Export Control Considerations

The academic culture is to share research results, data, and techniques broadly. It is important to consider that sharing unpublished findings involves risks as they can be used by a competing lab to advance a first publication of similar work. In addition, public disclosures of unpublished findings could affect securing IP rights to the research results.

Risks vary depending on the nature of the work. Each lab should conduct a risk-based analysis of their research and establish standards for sharing unpublished data that are communicated to every lab member, including when, why and how it can be shared. Any sponsor data sharing restrictions should be clearly communicated to lab members.

Engaging with Organizations or Individuals on U.S. Restricted Lists

The U.S. government maintains a list of individuals and institutions you are prohibited from doing business with, including sharing data or materials, unless the government gives you permission. It is important to request that your institution screen your potential collaborator against U.S. restricted and prohibited party lists prior to further engagement. Contact your export control office or official to screen potential collaborators. [Add Email of Export Control Officer or Office] For broader research security considerations on engaging with foreign collaborators contact your research security officer or office. [Add Email of Research Security Officer or Office]

Violating U.S. export control laws and regulations

It is important to know whether what you are sending requires an export license to the country you wish to send it to. If your work has dual commercial and military or proliferation applications, the U.S. government may require an export license before you send anything, including data, to researchers in another country. Don't forget that sharing data electronically can also be considered an export. Consult the export control official if you have questions about exports.

Ensuring Visitors Cannot Inappropriately Access Restricted Technology, Equipment, or Information

If you're working with restricted technology, equipment or information in your lab or elsewhere on campus you should have adequate protections in place consistent with sponsor and federal requirements. Visiting students and scholars should only have access to information related to and needed for the completion of the collaboration. All research security incidents should be reported to your institutions research security team immediately.

[University Name] Resources

Research Security

Questions about research security, such as engaging with international research collaborators, participating in research and related activities internationally, or requests for risk mitigation plans, should be addressed to [Add Email of Research Security Officer or Office]

Conflict of Interest (COI)

Questions regarding COI should be sent to [Add Email of Institutions COI Contact or Office]

Export Controls

Questions regarding export controls should be sent to [Add Email of Export Control Officer or Office]

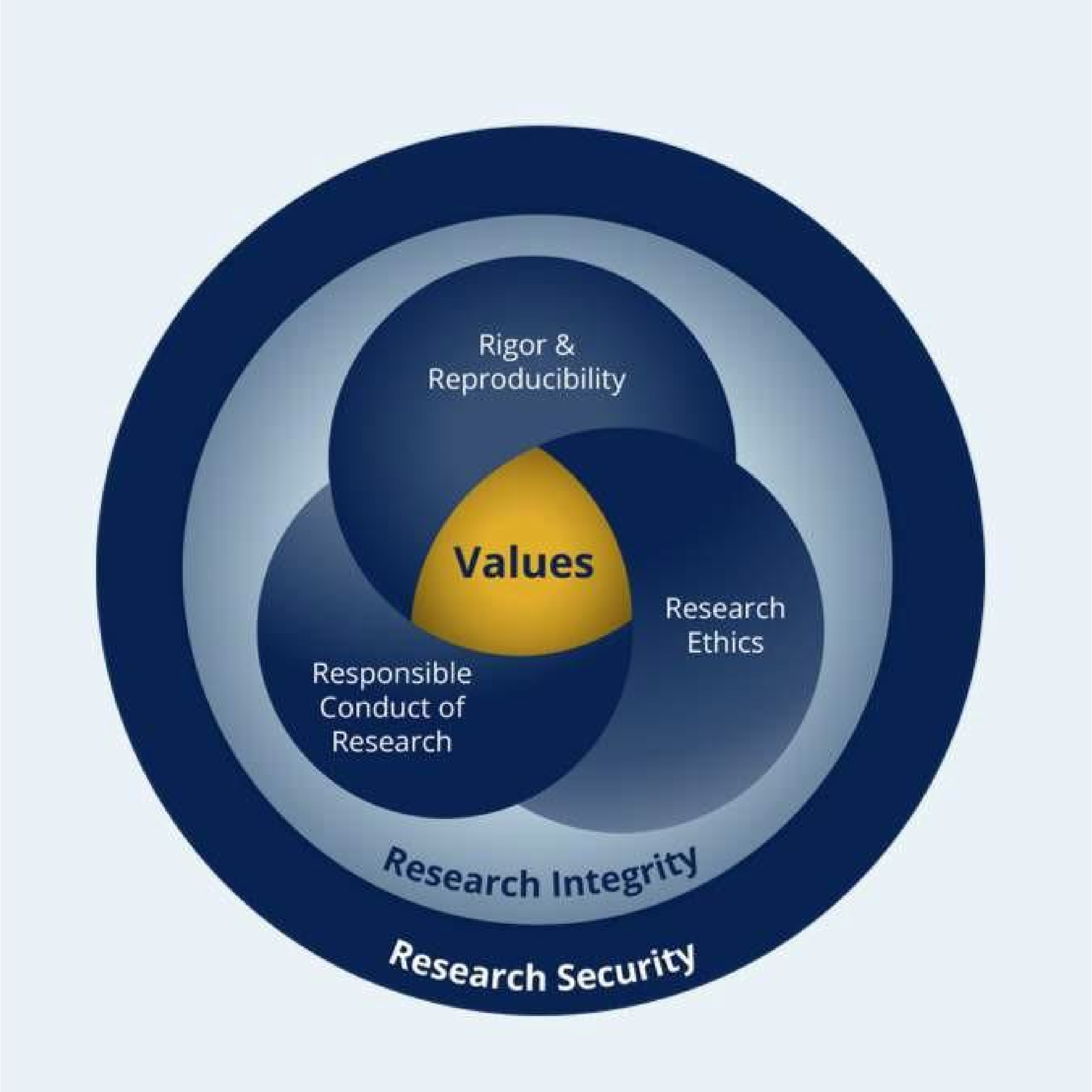
Research Security for Non-Senior/Non-Key Personnel

Research Security Overview

Research security is about safeguarding the research enterprise against the misappropriation of pre-published/pre-patented research and development (R&D) to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

Core Values

Research security includes components such as 1) adherence to regulations, policies, and procedures, 2) protection against intellectual property (IP) theft, misuse and unauthorized access to pre-published and pre-patented information, and 3) mitigation of research security risks. Research security also includes ethical research practices and working with integrity. This is exemplified in three fundamental areas of research. Responsible conduct of research, rigor and reproducibility, and research ethics. The core values that support these principles are the topic of the rest of this section.



Review the following core values and then read through the scenarios that follow and consider whether the actions described are consistent or inconsistent with these values.

Openness and Transparency

Openness and transparency mean making all relevant research data available to reproduce, verify and expand the science, reinforcing scientific objectivity. The U.S. research community values openness and transparency to build a better tomorrow with partners around the globe. Research security policies and procedures need to balance a free and open exchange of science and limit that exchange in situations of national interest or fairness.

Accountability and Honesty

Accountability and honesty play a role at several levels. Since the U.S. government funds a large portion of the research enterprise, researchers are accountable to taxpayers and to Congress. They are also responsible to their students, department or program, institution, and field of research. Validating work and justifying reasoning supports integrity.

Impartiality and Objectivity

Impartiality and objectivity play a significant role in research. A commitment to impartiality means scientists conduct their work without bias or preconceived notions, allowing them to approach their research objectively. When researchers succumb to personal beliefs, preferences, or external influences, it compromises the integrity and validity of their research and threatens U.S. research security.

Respect

Respect is the fundamental belief in a person's right to be heard and have opportunities. When respect is exercised in the scientific community and within a science team, it recognizes professional and personal differences, understands their significance, and capitalizes on attributes and qualities each person brings to the workplace.

Freedom of Inquiry

Freedom of Inquiry is a core tenet of research integrity. It allows the individual scientist to decide on an appropriate line of investigation and direct or dictate the choice of a research project. Academic researchers are experts in their field and interference from non-specialist or non-academic authorities is likely to adversely influence the outcomes.

Reciprocity

Reciprocity is the even exchange of ideas and knowledge. It embodies fairness and respect and demonstrates cooperation among many entities. Reciprocity also advances global problem solving, shares financial costs and resources, and encourages peace building through government cooperation. In return for public funding, disseminating knowledge becomes a crucial responsibility of researchers.

Merit-based Competition

Merit-based competition is the essence of the American research enterprise. Every agency strives to review proposals fairly, competitively, transparently, and in-depth. This ensures proposal evaluations are based on their intellectual value and not on personal relationships, improper influence, or unethical incentives. The evaluation of proposals and resulting awards must be based on their value to science, taxpayers, and to our nation’s economy and security. Non-discrimination is an important consideration in upholding these values and scientific excellence. Per the CHIPS and Science Act, each Federal agency shall ensure that research security policies and activities are developed and implemented in a manner that does not target, stigmatize, or discriminate against individuals on the basis of race, ethnicity, or national origin.

Scenarios

1. Dr. Patel collaborates with researchers at an overseas institution. They maintain a joint secure data-sharing platform, ensuring both parties have real-time access to research progress. Any published work cites contributors from both teams. Both institutions are informed of the arrangement.
   Is this collaborative arrangement consistent or inconsistent with the core values of the U.S. research enterprise?
   □ Consistent [Correct Response]
   □ Inconsistent
2. Dr. Stevens, a well-respected researcher in his field, is approached by a foreign organization offering substantial financial support for an ongoing project. The organization's website contains no information regarding its own funding sources, and these are never disclosed in communications. In exchange for its support, the organization requests exclusive rights to Dr. Stevens' research findings and asks Dr. Stevens not to disclose this partnership to his home institution. Dr. Stevens agrees, and accepts the funding without informing his home institution.
   Are Dr. Stevens' actions consistent or inconsistent with the core values of the U.S. research enterprise?
   □ Consistent
   □ Inconsistent [Correct Response]
3. Dr. Amin receives an intriguing research proposition from a foreign agency, involving a new project. Before moving forward, he discloses the opportunity to his institution and ensures new commitments do not conflict with existing obligations. While his institution identifies a potential conflict

with one project, Dr. Amin works with administrators to report activities regularly, managing potential conflicts. Dr. Amin then proceeds with the agreement.

Is Dr. Amin's approach consistent or inconsistent with the core values?

□ Consistent [Correct Response]

□ Inconsistent

4. Dr. Rivera is invited to give a presentation at an international conference regarding her recently published research. In her presentation, she openly credits all collaborators and funding sources in her talk. She also receives an honorarium—a monetary gift, from the conference organizers.

   Is Dr. Rivera’s approach to attending and presenting at the international conference inconsistent or consistent with the core values?

   □ Consistent [Correct Response]

   □ Inconsistent

5. Dr. Wilson, having heard of complications from international collaborations, is hesitant to partner with Dr. Nakamura from Japan, a leading expert in their mutual field. Despite knowing Dr. Nakamura's renowned reputation for integrity and the potential benefits from the collaboration, Dr. Wilson bypasses the opportunity, worried about the "hassle" of disclosure paperwork and the optics of working with foreign colleagues.

   Is Dr. Wilson's decision consistent or inconsistent with the core values?

   □ Consistent

   □ Inconsistent [Correct Response]

Potential Research Security Threats

Open and mutually beneficial partnerships between U.S. researchers and their international counterparts enable breakthrough innovations and significantly contribute to U.S. economic growth. The goal of this training is to help you be aware of and understand how to assess and manage potential risks of international collaborations and safeguard research.

The following topics explore potential risks and mitigation strategies.

Participating in an International Conference

Safeguarding IP and Other Protected Information

IP can refer to either innovations that the law protects from unauthorized use by others, like patents or copyrights, or raw data and information unprotected by law but subject to institutional ownership. To protect IP or unpublished results, it is critical that access to data is carefully managed. Non-public research findings that could be commercialized should not be discussed with anyone who is not part of the research project or where there is not an agreement with a trusted colleague.

Protecting Data When Traveling Internationally

Be sure to take security precautions to protect your data. You should assume that any of your devices may be accessed by others without your permission while traveling. The following are important considerations for protecting data while traveling internationally. To keep your data safe while traveling:

Leave behind any devices or media that are not absolutely necessary. If possible, obtain a clean laptop with encryption. If not, inventory and back-up your data and check for malware. Bring only the information and data you need for your trip. Do not retain sensitive personal information, whether yours or others, on your device. Your devices may be subject to search and seizure when you cross international borders or be compromised at your hotel.

Be mindful of potential data monitoring and theft of information on electronic devices, including flash drives. Keep your device with you and physically secure. Use a secure internet connection and turn off wi-fi when not in use. Do not download or transfer data or software to your device. A virtual private network should be used when connecting to hotel internet to diminish risks of data theft. Check with the export control and research security offices for country specific restrictions on use of VPN.

Do not use thumb drives given to you. Assume any removable media that doesn't belong to you is compromised. Do not use your own thumb drive in a foreign computer. Clear your web browsing history, utilize multi-factor authentication, and use a new password during travel and change it on return. Institutional servers should not be accessed on public computers that could capture login credentials. Access additional resources on traveling internationally with technology.

Violating U.S. Export and Sanctions Regulations

U.S. law makes the unauthorized export of some technologies and tools a crime. While it is unlikely that there will be issues with bringing your laptop and phone, you should be aware of any limitations on the export of software or data on your device. For a limited set of sanctioned countries, individuals, and organizations, including foreign universities and research institutes, export licenses may be required before you travel. Consult your institution's export control official if you have questions about exports.

Sharing Data or Materials with International Collaborators

Organizations and Individuals on U.S. Restricted Lists

The U.S. government maintains a list of individuals and institutions you are prohibited from doing business with, including sharing data or materials, unless the government gives you permission. It is important to request that your collaborator or a host institution or organization be screened against U.S. restricted and prohibited party lists prior to further engagement. Contact your export control office or official to screen potential collaborators. [Add Email of Export Control Officer or Office] For broader research security considerations on engaging with foreign collaborators contact your research security officer or office. [Add Email of Research Security Officer or Office]

Safeguarding IP and Protected Information

To protect your intellectual property (IP), including unpublished data and information, work with your sponsored projects or tech transfer officials to put confidentiality, data use or material transfer agreements in place before sharing data or materials externally. It is also important to remember that data sharing should be consistent with data management and sharing plans and participant consent if sharing data about human research participants.

Violating U.S. Export Control Laws and Regulations - Shipping

It is important to know whether what you are sending requires an export license to the country you wish to send it to. The US government may require an export license before you send anything, including data, to researchers in another country. Don't forget that sharing data electronically can also be considered an export. Consult your institution’s export control official if you have questions about exports.

Ignoring the Destination Country’s Import Laws and Regulations

Depending on what you are sending, particularly if you are shipping plants, animals or microbes, the country you are sending the materials to may require an import permit. Consult your institution’s export control official if you have questions about exports.

Collaborating with International Visiting Scholars at U.S. Institutions

Ensuring Visitors Cannot Inappropriately Access Restricted Content

If there is restricted technology, equipment, or information in your lab or elsewhere on campus adequate protections should be in place consistent with sponsor and federal requirements. Visiting students and scholars should only have access to information related to and needed for the completion of the collaborative work. All security incidents should be reported to the University’s security team immediately.

Collaborating Abroad

Participation in a Foreign Talent Recruitment Program

Any risks associated with an overseas opportunity need to be assessed and managed. A primary consideration is ensuring that the opportunity is not a malign foreign talent recruitment program, which would prohibit you from receiving US federal research funding. Many countries, or entities within countries, sponsor talent recruitment programs for legitimate purposes.

Malign Foreign Talent Recruitment Programs

Unfortunately, some programs require participation in activities that create conflicts of interest or commitment and could be unethical or even illegal. These are referred to as “Malign” Foreign Talent Recruitment Programs (MFTRPs). The CHIPS and Science Act of 2022 prohibits grant awardees, including universities, individual investigators, and other key personnel, from participating in these malign programs. Participation will result in your being ineligible to receive or be supported by federal research funding and could impact future funding opportunities.

Central concerns about MFTRPs include terms that result in overlap or duplication of U.S. funded research, unauthorized transfer of unpublished U.S. research data, methodology, and IP, and over-commitment on U.S. funded projects due to engagement in undisclosed international activities, among others. A program is considered malign when these and other features are present, and the program is sponsored by a country of concern; currently China, Russia, Iran and North Korea.

Federal Agency Risk Reviews of Fundamental Research Proposals

Although foreign talent recruitment programs that don't include malign terms as well as other types of international appointments or engagements are not explicitly prohibited, a number of federal research funding agencies are considering potential risks associated with international engagements during review of fundamental research proposals. Agencies that have published information on their risk review processes include the Department of Defense (DOD), Department of Energy (DOE), National Science Foundation (NSF) and National Institutes of Health (NIH).

Details can be found in individual agency guidance and an overview on the SECURE Center website. Areas of commonality include concerns about engagement with entities and individuals on U.S. restricted lists and a focus, whether explicitly noted or not, on critical technologies. Factors cited by DOD and DOE also include foreign funding, in particular from countries of concern, and concerning behaviors associated with patenting.

Conflicts of Interest, Conflict of Commitment and Disclosure

NSPM-33 defines a conflict of interest (COI) as a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.

This definition and process differs from conflict of commitment (COC). A COC is a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicts of time and effort, including obligations to dedicate time in excess of organizational or research agency policies or commitments. If a researcher makes commitments that exceed 100% of their available effort, whether at the same institution or other entities with which they hold affiliations, they have a conflict of commitment.

Another type of COC is the obligation to improperly share information with, or to withhold information from, an employer or research agency, which may threaten research security and integrity.

In addition to their obligations to report to the University, researchers separately must disclose all activities, affiliations, and sources of support for any of their research endeavors, regardless of whether they are made available through a researcher's home institution or directly to the individual, or have monetary value, through biosketch and current and pending (other) support forms to various sponsors. This reporting includes certain "in-kind resources" (e.g., office/ laboratory space, equipment, supplies, or employees with external funding). Disclosed information in the Biosketch and Other Support forms helps a sponsor to assess an individuals' qualifications and capacity to perform the proposed and ongoing research, any overlap with other obligations and duplication of research, and view any potential conflicts of interest and commitment. [Option to Add Link to Institution's Disclosure Webpage Here]

Disclosure is essential for the furtherance of the U.S. research community. It has a central role in creating a trust-based research culture, creates a level playing field for all involved, and carries significant consequences for individual researchers, organizations, and the nation as a whole.

[University Name] Resources

Research Security

Questions about research security, including engaging with international research collaborators, participating in research and related activities internationally, or requests for risk mitigation plans, should be addressed to [Add Email of Research Security Officer or Office]

Conflict of Interest (COI)

Questions regarding COI should be sent to [Add Email of Institutions COI Contact or Office]

Export Controls

Questions regarding export controls should be sent to [Add Email of Export Control Officer or Office]

Interested in the full Research Security and Disclosure Training?

Click here to take the training [Or add University Link].