

Research Security Training - Audio Transcript

1. Course Introduction

1.1 Course Introduction

Welcome to research security training. This training, developed by several research universities, condenses and combines federal modules 1-4.

1.2 Module Information

Select each button to the left as needed to learn more about how to navigate through the module and adjust settings to meet your needs.

Navigation:

Select the next and previous arrows to navigate through the course. Use the on-screen controls to control the video.

Glossary:

Select the menu icon to access the glossary. Once inside the glossary, use the scroll bar to navigate.

Closed Captioning:

This training includes various videos. To make it accessible for everyone, we've included closed captioning in each video. Select the CC button below the video to enable closed captioning.

Sound:

This lesson contains audio narration. You will need speakers or headphones. Select the playback speed control to speed up or slow down audio.

2. Router

2.1 Begin Training

Select any available section to continue.

3. Section 1

3.1 Section 1: Introduction to Research Security

Section 1: Introduction to Research Security.

3.2 Objectives

By the end of the training, learners will be able to:

Define research security within the context of their work and the research enterprise. Identify the key federal government guidance impacting research security. Recognize that all stakeholders contribute to research security. Identify the core values of academic research and how undue foreign influence threatens the research community. Recognize situations that may indicate undue foreign influence.

3.3 Scenario Introduction

Hi there! I am Vanessa and I'm your guide for this training. I would like for you to meet two team members, Sameer and Fatima.

Sameer:

I'm Dr. Sameer Tanesha. I'm a postdoctoral researcher and a member of Dr. Kiani's research group.

Fatima:

I'm Dr. Fatima Kiani, an assistant professor.

3.4 Meet Sameer and Fatima

Fatima:

Hi Sameer! How's your week going?

Sameer:

Good. But our research administrator, Emily Green, reached out about our project. She thinks there's potential for some research security concerns.

Fatima:

I'm attending a research security conference. You should come too!

Sameer:

The conference is about safeguarding research and protecting our information and intellectual property from theft.

Fatima:

I'm looking at the conference app now. It says that research security is about the principles and actions that protect the research enterprise from misappropriation, violations of research integrity, and foreign government interference.

Sameer:

By practicing research security, we safeguard information, data, technological advancement, and US economic and national security.

Fatima:

If researchers protect their pre-publication work the US will continue to inspire innovation, encourage investment in research and development and maintain a culture of trust and collaboration.

3.5 Knowledge Check

What are the benefits to research security? Choose all That Apply.

Incorrect:

Incorrect. The benefits of research security are maintaining trust, protecting economic security, safeguarding data, and nurturing innovation.

Correct:

Correct! Research security has many benefits including maintaining trust, protecting economic security, safeguarding data, and nurturing innovation.

3.6 Keynote Transition

The keynote speaker is about to define research security and how it is influenced by the federal landscape.

3.7 Keynote Introduction Video

Rachel:

Hi there, I'm Rachel Painter a Vice Chancellor for Research. One of my office's responsibilities in protecting research is to set policies and procedures to prevent the misuse of research funds.

3.8 Keynote Address

Rachel:

Research in the United States is remarkable, driven by a robust federal funding system, and world-class universities, and institutes. Research advances knowledge, enhances medical treatments, and fuels technological progress. Our research system promotes innovation, collaboration, job creation, and economic growth.

Unfortunately, other nations seeking to emulate the US research ecosystem may seek to obtain ideas, inventions and investments through illicit means. This can impact researchers' careers and the national and economic security of the US. We stand at a critical juncture where protecting our research has never been more crucial.

3.9 Defining Research Security

So, what exactly is research security? Think of it as the collective system of controls that safeguards the research enterprise against threats to national and economic security integrity. This includes regulations, policies and procedures that protect the research enterprise from theft, misuse and unauthorized access. It also mitigates insider threats and foreign influence.

Ethical Research Practices:

Ethics serve as a barrier to engaging in deceptive practices such as intentionally failing to disclose financial or other relationships, particularly those outside the country.

Research Security Components:

Research Security Components is the set of regulations, policies, and procedures that protect the research enterprise from IP theft, misuse, an unauthorized access. It also mitigates insider threats and foreign influence.

3.10 Everyone Is Responsible

Every one of us chairs responsibility for maintaining security. Our collective efforts help you protect unpublished work intellectual property and reputations. Our commitment will retain our culture of innovation trust and collaboration and ensure good stewardship of sponsored funds.

3.11 Key Federal Regulations

Recently, four key federal guidance has been issued. These are JASON report, National Security Presidential Memorandum, NSPM-33 Chips and Science Act, and the Research Security Programs Guidelines.

Click on each guidance document for more information.

JASON Report:

The 2019 JASON Report Fundamental Research Security, commissioned by the National Science Foundation, fully supports open access to fundamental research and emphasizes the value of international collaboration. It asserts research integrity requires full disclosure of all actual or potential conflicts of interest. It also recommends NSF and recipients investigate and adjudicate non-compliance issues.

NSPM-33:

National Security Presidential Memorandum. NSPM-33 calls on federal research funding agencies to identify shared disclosure requirements, incorporate persistent identifiers, PIDs, and require a research security program at recipient organizations receiving more than \$50 million annually in federal research funding. NSPM-33 also seeks consequences for non-disclosure and provides guidance for sharing information on violations across federal research funding agencies.

CHIPS and Science Act of 2022:

The chips and science act boost investments in R and D and mandates the NSF establish a research security and integrity information sharing and analysis clearing house for all stakeholders, develop a risk assessment, and provide research security training as a part of responsible and ethical conduct of research RDCR training. They act defines and directs agencies to prohibit membership in malign talent recruitment programs.

Research Security Programs Guidelines:

The NSPM-33 implementation guidance provided additional clarity on research security program requirements including details on training requirements, foreign travel security, and cyber security. Final guidelines were published on July 9, 2024, for agency implementation.

3.12 Personal and National Benefits

Rachel:

We've established what research security is, the regulatory landscape, and why it matters. Now we will explore the considerable personal and national benefits.

Sponsors must have faith that funds are appropriately and judiciously employed. It is critical that researchers disclose all support to allow agencies to make informed funding decisions.

Our adversaries are sophisticated. Be vigilant in vetting collaborators and sharing information. When you do this, you benefit by maintaining your reputation and results.

You deserve to communicate your results in the time format and place of your choosing. Securing your results, innovations and intellectual property are directly correlated with career advancement.

In addition, our national security interests are advanced when we are active participants in keeping sensitive information out of the reach of our adversaries, maintaining technological advantages and protecting lives.

Interfering foreign governments engage in data theft and corruption with principal investigators, research teams and organizations.

3.13 Core Values of Academic Research

Fatima:

Hi Sameer, Dr. Painter's keynote address provides a great backdrop for our next topic, Core Values. Research security depends upon investigators, administrators and institutions 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 three principles is the topic of this interactive poster. They include openness and transparency, accountability and honesty. Impartiality and objectivity, respect, freedom of inquiry, reciprocity, and merit-based competition. Look into these core values for more information.

Sameer:

Great, I'm looking forward to learning more.

Openness and transparency:

Openness and transparency mean making all the relevant research data available to others 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. However, this core belief leaves U.S. research vulnerable to bad actors. 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 the taxpayer and Congress. They are also responsible to their students, department or program, institution, and field of research. When investigators are dishonest in their research and not answerable to all its stakeholders, the U.S. research enterprise is at risk. Researchers must validate their work and justify their reasoning. In return for being honest, researchers gain credit for their work which builds their reputations.

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 exist, to be heard, and to have the same opportunities as everyone else. 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, particularly from external and non-academic constraints.

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 the intellectual value, and not on personal relationships, improper influence, or unethical incentives. Proposals and the resulting award must be based on value to the science, the taxpayers, and to our nation's economy and defense.

3.14 Knowledge Check

How do you achieve research security? Choose all that apply.

Incorrect:

Hmmmm. That's not the right answer. You achieve research security through safeguarding data, intellectual property and sensitive information; by complying with regulations and best practices; and by ensuring research is conducted consistently with the community's core values and ethics.

Correct:

Great work! You achieve research security through safeguarding data, intellectual property and sensitive information; by complying with regulations and best practices; and by ensuring research is conducted consistently with the community's core values and ethics.

4. Section 2

4.1 Section 2: The Importance of Disclosure

Section 2: The Importance of Disclosure

4.2 Section Overview

Now that Fatima has a better understanding of Research Security, she plans to visit Emily at the Office of Sponsored Research to learn more about the disclosure process. As Fatima visits Emily, we will learn the importance of full disclosure and how disclosure can build trust. In this section, learners will understand what disclosure is and be able to comprehend how disclosure is a means to report potential conflicts of interest and conflicts of commitment. And finally, learners will understand the importance of full disclosure and its central role in a trust-based research culture. Now let's join Fatima as she makes her way to meet Emily in her office.

4.3 What is Disclosure?

Click the buttons for answers to Fatima's questions about disclosure.

What is Disclosure?:

It is important to be candid and forthcoming in our disclosure, even if what's asked doesn't seem relevant to us. It is relevant to the funding agencies. It also helps uphold one of the critical shared values

of the US research enterprise, transparency. Some examples of information all senior and key personnel are asked to disclose are sources of funding or support, outside employment, business ownership or a significant stake in a company, collaborations, appointments and affiliations. Current and pending sources of research funding and travel in connection with academic and professional aims.

How is Disclosed Information Used?:

If you don't mind me asking, how is the disclosed information used?

4.4 COI vs. COC

Fatima:

You mentioned that one of the uses for disclosed information is to identify conflicts of interest and conflicts of commitment. I've heard those two terms before, but to be honest I've noticed that people have used them interchangeably and it's only left me more confused.

Emily:

You aren't alone. That's why our office provides additional resources. Let's learn more.

What is a Conflict of Interest?:

I think that's a great idea.

That reminds me of a story I heard when I was a postdoc about a researcher who studied a drug made by a pharmaceutical company in which they owned stock. It bothered me because the researcher had a financial stake in the company's success, which may have caused bias in how they interpreted their research results.

That's a good point and exactly why institutions implement conflict management plans in these types of situations that include requirements like disclosing the outside interest to human subjects in consent documents and in publications and presentation.

What is a Conflict of Commitment?:

Can you explain what a conflict of commitment is?

Sure. Of the two types of conflicts, conflict of commitment tends to be the most confusing. A conflict of commitment 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 conflicting commitments of time and effort, including obligations to dedicate time in excess of organizational or research agency policies or commitments. Other types of conflicting obligations including obligations to improperly share information with, or to withhold information from an employer or research agency, can also threaten research security and integrity and are an element of a broader concept of conflicts of commitment. Somewhere in your contract and or funding awards, you committed to a certain amount of time and effort. This effort is usually represented as a percentage of time or months of effort. If a researcher makes commitments that exceed one hundred percent or twelve months in their current and pending support form whether at the same institution or other entities with which they hold affiliations, they have a conflict of commitment. Other types of conflicting obligations, including obligations to share information improperly, or to withhold information from an employer or funding agency, can also threaten research security and integrity and are an element of a broader concept of conflicts of commitment.

4.5 Benefits of Disclosure

Emily:

That's a great question. There are different ways disclosed information can be used: For example, disclosed information can be used to properly assess an individual's qualifications and capacity to perform the proposed or ongoing research and prevent overlap with other obligations. Disclosed information can also be used to avoid duplication of research and assess potential conflicts of interest and commitment.

Fatima:

It's all making more sense now. Disclosing information is really important, because it helps assess potential conflicts of interest and determine if there are ways to manage those conflicts. It also gives me an opportunity to be able to show off everything I've been working on.

4.6 Transition to Activities to Disclose

Thanks to Emily, Fatima now has a greater understanding of the disclosure process. However, she still needs to learn which activities need to be disclosed for her upcoming research project. In this section, we'll focus on Understanding the types of activities which must be disclosed throughout the award lifecycle and how to disclose. Learners will understand types of activities which must be disclosed throughout the federal award lifecycle and that federal agencies have specific disclosure requirements. In addition, learners will learn where to locate current information on disclosure requirements. Now, let's see if Emily has some resources Fatima can use as a guide on what types of activities she must disclose.

4.7 Activities, Affiliations, and Support to be Disclosed

Fatima:

Emily, now that I better understand the importance of complete disclosure, can you walk me through what types of activities I need to disclose? I plan to share this with my team so we're prepared for the proposal process.

Emily:

Absolutely. It is important to fully understand what needs to be disclosed.

4.8 How to Disclose

Click the buttons to learn more about how to properly disclose.

4.9 Conclusion

Fatima:

Thanks for the information, these resources were really useful. I'm thinking this is information I should share with my team to make sure everyone is on the same page.

Emily:

I think that's a great idea.

4.10 Knowledge Check

4.11 Non-disclosure

The office of Sponsored Research has been a big help in supporting Fatima during the disclosure process. To ensure her team's success, Fatima is preparing to brief her research team on the importance of disclosure, but she still needs a little bit more information. In this section, learners will gain a solid understanding of various types of problematic behaviors that can undermine research security. Let's meet up with Fatima as she is preparing for this brief.

4.12 Behaviors that Negatively Impact Research Security

Rachel:

Hey Fatima, it's nice to see you! How's the research project going?

Fatima:

Hi Dr. Painter. It's going well. I've been working closely with Emily in the sponsored research office who help me better understand disclosures. I'm actually preparing a brief for my team on some of the important points.

Rachel:

That's great. Did you see the materials our research security office just put out to the university? It is a great resource. You might want to review them. I think it would help the you and the team understand the behaviors that could impact research security.

Fatima:

Thanks, that's a great idea!

Rachel:

No problem. Glad I can help. I have to run but keep up the good work.

4.13 Case Study

Fatima:

Hmmm ... it looks like the office of Research Security posted some resources on their website. I should check them out.

Case Study (Video):

The following case study is based on true events about how a lack of disclosure can lead to severe consequences.

In 2020, an American educated faculty member and researcher at a Texas University was arrested on conspiracy charges, making false statements and wire fraud.

The faculty member was a US citizen and full professor in the Department of Chemical Engineering and was engaged in federally funded research partnerships with NASA.

He was a principal investigator with his research team receiving nearly \$750,000 in grant funds.

NASA grant proposal regulations require principal investigators to submit a biographical sketch and disclose current and pending support information for any grant proposal. The researcher repeatedly and deliberately made false statements and submitted false and misleading information regarding his employment, affiliation, intended collaboration with foreign universities and corporations thus violating both the pre-award and performance requirements of the NASA grant. On repeated occasions, the researcher falsely certified compliance with NASA.

The University maintains a policy requiring employees to disclose conflicts of interest. The policy states members have a responsibility to identify and manage reduce or eliminate conflicts of interest that may arise due to financial or other personal interests of an investigator; requiring employees engaged in research to identify all research or research activities in which the investigator is engaged at the time the financial disclosure statement is submitted. The University requires faculty and staff to submit a financial disclosure statement upon hire and subsequently on an annual basis; requiring employees to disclose conflicts concerning outside employment and significant financial interests.

This faculty member hired in 2004 did not disclose his research or any financial conflicts of interest under the University's policies and procedures. Following a federal investigation, the researcher was found to have collaborated with entities supporting foreign governments and was arrested by the Department of Justice. Among the associations the researcher deliberately concealed were his participation in a foreign talent program and his service as director of a foreign institute, which posed a

threat to national security. Shortly after his arrest, he was terminated from the University. He later pled guilty to violating NASA regulations and falsifying official certificates or writing, both violations of the US code.

The researchers served jail time and was required to pay a \$20,000 fine and over \$86,000 dollars in restitution to NASA.

4.14 Section Wrap-Up

Fatima:

These research security resources and that case study really helps me understand the importance of disclosing properly. There are some pretty serious consequences if we don't get it right. I need to make sure that I share this with my team.

4.15 Knowledge Check

4.16 Overview - Consequences

For additional information on topics related to sharing data and materials, click the buttons of interest to the left.

4.17 Consequences

Fatima:

Funding agencies are actively searching for conflicts of interest and commitment and risks associated with unreported foreign affiliations. Many applicant organizations are also proactively working to verify information provided.

Consequences to an Individual?:

If a researcher intentionally fails to properly disclose, there are more severe consequences. Some consequences for individual researchers include facing civil monetary penalties for intentional omission under the inspector general act, they can face suspension and debarment, which would prevent them from participating in contracts or awards with the federal government. Additionally, individual organizations might prohibit an individual's involvement in other activities including peer review, submission of applications, or joining other award submissions. Such consequences would severely impact a researcher's career and professional reputation.

Consequences to an Organization?:

Yes, you are right, Sameer. But it's even bigger than that. Not only would our team be impacted, but so could our institutions. Let's talk about what consequences organizations might face. Let's remember that a researcher's organization certifies to the federal government that all information within an application is current, accurate and complete. The organization relies on the disclosures of the researcher. However, organizations themselves must also do their due diligence. Federal funding agencies, corporate partnerships, and State funding expectations involve transparent and reciprocal partners who take

research security and intellectual property protection seriously. Along with significant reputational risk and loss of intellectual property, organizations risk additional conditions and administrative consequences if material undisclosed information is identified. These risks can be costly to the organization due to a loss of valuable information, lost benefit of innovation investment, and expenses associated with investigation and additional oversight requirements. If the non-disclosure is found to be material or substantial, the organization is at risk of termination, pause, or withholding of funding. Financial penalties, loss of eligibility for future funding, and legal consequences are all potential consequences for the organization.

Consequences to the U.S. Research Enterprise?:

That's a great question Sameer. The US research enterprise is a major stakeholder that is somewhat forgotten as we work to address conflicts of interest, conflicts of commitment, and malign influence. The U.S. research enterprise is responsible for many of the most significant innovations in history, bringing economic value and benefit to humanity. That's why the continual loss of basic and applied knowledge at the hands of malign actors is a growing risk which can lead to increased burden. This loss reduces the efficiency of our processes and can bring increased oversight, reporting requirements, and greater limits on collaboration. Ultimately, this brings second-order effects, leading to the loss of research outcomes, and making it more challenging to recruit top talent. In the end, this works to erode U.S. innovation capacity. When we look at the bigger picture, 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.

5. Section 3

5.1 Section 3: Risk Mitigation and Management

Section 3: Risk Mitigation and Management

5.2 Objectives

By the end of this training learners will be able to identify types of international collaborative research and professional activities and the potential risks of each. Describe resources to assess potential risks associated with international activities. Identify strategies and best practices for managing and mitigating potential risks of international activities.

5.3 Introduction

Open and mutually beneficial partnerships between US researchers and their international counterparts enable breakthrough innovations and significantly contribute to US economic growth. Our goal is to help

you be aware of and understand how to manage the potential risks of international collaborations. This will help you safeguard research. Let's begin with giving a talk internationally.

5.4 Scenario 1: Giving a Talk Internationally

Giving a talk internationally, select begin to access the scenario.

5.5 Scenario 1: Introduction

Dr. Fatima Kiani received an email inviting her to present her work at an upcoming international symposium being hosted in another country. What else should she think about before traveling abroad and sharing her research results with the international community? Select next to learn more about potential risks and how to manage them.

5.6 Scenario 1: Possible Risks

Select each button to learn about the potential risks of giving a talk internationally. After you review all potential risks select next to continue.

Traveling without required sponsor approval:

Traveling without required sponsor approval. Your sponsor may require prior approval before you travel abroad. Be sure to read the terms of your awards to find out if there are any applicable travel preapprovals or restrictions.

Theft of data:

Theft of data. You may not think your data are particularly vulnerable, but other people or organizations might not agree - and try to steal it. Make sure you take security precautions appropriate for your destination and type of data. You should assume that any of your devices may be accessed by others without your permission while traveling.

Sharing restricted information:

Sharing restricted information. Sponsors may restrict distribution of some research information. Again, the terms and conditions of your award will identify any restrictions on information sharing that may affect your ability to freely share your research data with others. If you're working on research where there are restrictions, make sure you don't share the data with others until you obtain permission from your sponsor.

Violating U.S. export & sanctions regulations:

Violating US export and sanctions regulations. US 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.

Threats to personal safety:

Threats to personal safety. Beyond these research specific risks, it is unfortunate but true that international travel, depending upon where you are traveling, may involve infrequent but real threats to personal safety.

5.7 Additional Resources

For additional information on topics related to giving a talk internationally, click the buttons of interest to the left.

5.8 Scenario 2: Sharing Data or Materials

Sharing data or materials, select begin to access the scenario.

5.9 Scenario 2: Introduction

Fatima's presentation was a success. One of the attendees approaches her to ask if she would share her data set and materials so they can evaluate the potential for a future collaboration. She suspects there could be risks associated with sharing data or materials and asks her mentor, a more experienced PI, for advice. Select next to learn more about potential risks and how to manage them.

5.10 Scenario 2: Possible Risks

Select each button to learn about potential risks of sharing data or materials. After you review all potential risks select next to continue.

Failure to protect intellectual property and other protected information:

Failure to protect intellectual property and other protected information. You want to protect your intellectual property. If you share data or materials before your institution has data use or material transfer agreements in place, you risk losing potentially valuable patent protections. You should also only share data consistent with your data management plan. If you have data about human research participants, any data sharing must be consistent with participants consent.

Violating U.S. export control laws and regulations:

Violating US export control laws and regulations. It is important to know what you are sending and whether it 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 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.

Ignoring the destination country's import laws and regulations:

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 were sending the materials to, may require an import permit. Their import rules can be different than US import rules.

Providing resources to a “bad actor”:

Providing resources to a bad actor. There is a small but real risk that you could be sharing data or materials with an individual or institution identified by the US government as a bad actor. Do you know who your international partner is? What do you know about both the person making the request and the institution they're associated with? Are they engaged in an area of research that may be sensitive? How would you know? The United States government maintains a list of individuals and institutions you are prohibited from doing business with including sharing data or materials with unless the government gives you permission. It is important to request that your institutions screen your collaborator against US restricted and prohibited party lists before you send them anything.

5.11 Additional Resources

For additional information on topics related to sharing data and materials, click the buttons of interest to the left.

5.12 Scenario 3: Collaborating on a Research Project

Collaborating on a research project. Select begin to access the scenario.

5.13 Scenario 3: Introduction

Collaborating on a research project. Fatima is now planning a collaborative international research project. What potential risks does she need to consider as they kick off the collaboration? Select next to learn more about potential risks and how to manage them.

5.14 Scenario 3: Possible Risks

Of course, as you move deeper into a collaborative relationship, you need to remain aware of issues we've discussed already; travel safety, export control, and IP protection. As your research collaboration ramps up and your team begins to produce results, there are things that the team does control that you need to think about and discuss. Select each button to learn more about the potential risks of collaborating on a research project. After you review all potential risks select next to.

Improper authorship attribution and other collaboration risks:

Improper authorship attribution and other collaboration risks. Research fields have different norms and traditions, particularly around attribution of authorship on publications, researchers in the same field but in different countries can have different norms and traditions. Without laying the groundwork for a common understanding of how your specific collaboration will work, different unexpressed assumptions can lead to conflict.

Conflicting national research integrity rules:

Conflicting national research integrity rules. You and your partners may be operating under different or even conflicting research integrity rules and expectations. Any differences need to be identified early in strategies developed to comply with them so that no participants run the risk of violating their national rules and requirements for research integrity.

Violating the terms of sponsored research agreements:

Violating the terms of sponsored research agreements. You could violate the terms of sponsored research agreements if you fail to disclose the foreign collaboration to your sponsor or obtain prior approval if needed. At the extreme these failures could require the return of funds or bar you from obtaining research funds from the US government in the.

Reputational risks:

Reputational risks. Individuals or institutions could suffer reputational damage if undisclosed engagements are discovered. The US research enterprise depends upon the public trust and negative publicity surrounding the inability to properly secure US government funded research or improper use of funds potentially violates that trust.

5.15 Additional Resources

For additional information on topics related to collaborating on a research project, click the buttons of interest to the left.

5.16 Scenario 4: Hosting International Students or Scholars

Hosting international students or scholars. Select begin to access the scenario.

5.17 Scenario 4: Introduction

A student of Fatima's international collaborator is incredibly skilled in one aspect of a needed experiment, but only Fatima has instrumentation they need for the analysis. They decide that the student should work in Fatima's lab for six to twelve months. Select next to learn about potential risks and how to manage them.

5.18 Scenario 4: Possible Risks

The arrival of a visitor is a time to touch base again on some of the issues we've discussed up to this point. Select each button to learn more about potential risks of hosting international students or scholars.

New members of the collaboration could be “bad actors”:

New members of the collaboration could be bad actors. Are there new members of the team for whom you may not have requested screening for presence on US restricted lists? If so, additional screenings should be conducted before moving forward.

The host lab’s intellectual property could be stolen or diverted:

The host lab's intellectual property could be stolen or diverted. Protect all data and intellectual property in your lab, not just the data and IP for the joint collaborative project. Fatima must protect information and data for other projects and ensure that our students and lab members are educated on how to maintain security of the projects they are working on. Particularly if they are sharing space or working with a visitor.

Visitors could inappropriately access restricted technology, equipment, or information:

Visitors could inappropriately access restricted technology equipment or information. If you're working with restricted technology equipment or information in your lab or elsewhere on campus, do you have adequate security protections in place? The visiting students should only have access to information related to and needed for the completion of the collaboration.

5.19 Scenario 4: Mitigation Strategies Animation

As a routine security practice, Fatima provided her institution the necessary information for screening the visiting student. Review sponsored research agreements for terms related to hosting visitors and obtain necessary approvals for commitments to host the student are made, the visitor will access projects other than the current collaboration. To ensure Fatima is aware of signs of potential loss, theft or diversion of intellectual property; she should consult with her institution regarding potential insider threat risks.

5.20 Additional Resources

For additional information on topics related to sharing data and materials, click the buttons of interest to the left.

5.21 Scenario 5: Accepting an Overseas Appointment

Excepting an overseas appointment. Select begin to access the scenario.

5.22 Scenario 5: Introduction

One of Fatima's collaborators approaches her with an offer of a joint appointment at their foreign institution. This will allow Fatima to set up a lab there, advise graduate students and postdocs and submit proposals directly to research agencies in that country. While the prospects of academic appointments in two countries at the same time is daunting, Fatima recognizes this is a rare opportunity. Fatima wants to make sure that she does not jeopardize her current academic appointment or her funding from US government agency grants. She schedules time to meet with Emily Green to discuss what she needs to think about in making her decision. Select next to learn more about potential risks and how to manage them.

5.23 Scenario 5: Possible Risks

Select each button to learn more about potential risks of accepting an overseas appointment. After you review all potential risks, select next to continue.

Participation in a foreign talent recruitment program:

Participating in a foreign talent recruitment program. Any risks associated with an overseas appointment need to be assessed and managed. A primary consideration is ensuring that the opportunity is not on the 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. To attract scientific talent, they offer financial incentives with a potential to relocate. Unfortunately, some programs in encourage or even require unethical and criminal behaviors.

You must fully understand the terms of any overseas appointment before you agree to them. For example, does the employment contract include requirements for publication in top tier journals or require that you list both the international and US affiliation on all the publications? Does it offer compensation for the establishment of a lab or company to accept a faculty position or undertake any other employment or appointment that duplicates activities the US is funding in your home lab? Does agreement require a greater commitment of effort than you have percent effort available in the US, or does it require secrecy about the existence of the recruitment program contract? A program is considered a maligned foreign talent recruitment program when these and other earning features are present, and the foreign talent recruitment program is sponsored by a country of concern; currently China, Russia, Iran and North Korea. Your institution may be able to assist you in determining whether your offer is coming from such a program or whether the terms of the agreement violate integrity principles, other US laws and regulations or terms of award.

Violating integrity principles, U.S. laws, or regulations:

Violating integrity principles, US laws or regulations. Fatima seeks advice from her institution on whether the terms of the agreement constitute a malign program and violate integrity principles, other US laws or regulations and what approvals might be needed to engage in the activity.

Violating your institution's policies:

Violating your institution's policies. Other risks include conflict with employment policies of your home institution, especially any policies about conflicts of commitment. Make sure that accepting that offer is consistent with all policies of your home institution.

Violating terms of federal sponsor requirements:

Violating terms of federal sponsor requirements. You should also review the terms of all active sponsor projects particularly those from federal agencies to make sure there are no limitations on a secondary or overseas appointment. Committing to more research effort than there is time available or committing to do the same work for multiple sponsors. Conflicts can arise if the new appointment over-commits your effort compared to effort already committed on current sponsored projects.

5.24 Scenario 5: Mitigation Strategies Animation

If you are offered the opportunity of a joint appointment, congratulations! First make sure that accepting that offer doesn't violate institutional and sponsor policies, especially policies on conflict of commitment before you sign the agreement. Make sure you request and have reviewed a certified translation of the document before signing. If the agreement is subject to laws of another country, do you understand those requirements and have the ability to comply? Ensure that an appointment does not overcommit your effort based on your effort on current sponsored projects. Report all foreign income to the IRS. And finally, if you are entering into any agreement in your personal capacity, rather than as an employee or faculty member of your current institution, have your personal lawyer review all documents to ensure compliance with your current employment agreements and with US laws and regulations.

5.25 Scenario 5: Risk Mitigation

5.26 Additional Resources

For additional information on risk mitigation and management, click the buttons of interest to the left.

6. Section 4

6.1 Section 4: International Collaboration

Section 4: International Collaboration

6.2 Introduction

Sameer:

I've got to admit. International collaboration seems to come with a lot of things to worry about. What if I make a bad decision and get into trouble? My work life is stressful enough already. Maybe I'll just stick to US only collaborations from here on out.

Fatima:

Don't do it Sameer. Trust me, working across borders is absolutely crucial to global scientific progress. So don't make the mistake of getting so worried about research security that you avoid working internationally with fellow scientists.

Sameer:

Hold on. So, you're saying that avoiding international collaboration because I'm afraid to make a research security mistake is even worse than making the mistake itself.

Fatima:

Exactly. As we'll see in this section even missteps can often be corrected if you know when and how to get help from your colleagues, supervisors and administrators, but shutting your door to the world prevents anything from ever happening.

6.3 Core Values in the International Context

Fatima:

Recall from the research security conference we attended, the discussion of working with integrity and the core values of academic research including openness and transparency, accountability and honesty impartiality and objectivity, respect, freedom of inquiry, reciprocity, and merit-based competition.

Sameer:

But how are a bunch of abstract words, like openness or respect, supposed to help me with real situations.

Fatima:

Good question. It's true. We talk about the core values through words, and those words are pretty abstract. These values evolve alongside the research enterprise, and they continue to evolve today. It isn't just cutting-edge labs or groundbreaking discoveries that make our research enterprise preeminent in the world. Alignment with the core values ensures that the whole ship is moving in the right direction.

6.4 Transparency and Reciprocity in International Scientific Collaborations

You'll have to make sound decisions based not only on what's good for your university, but for the broader US research enterprise, including federal research funding agencies. Are you ready to put the core values to work?

6.5 Assessing International Collaborations

In the rest of this part, we'll explore some specific examples of international collaborations using five hypothetical situations. The object here is simple, read each hypothetical and then decide whether the situation is consistent with the core values of research integrity or inconsistent with those values. The core values are more about developing your instincts than holding to precise definitions. The key here is to pay attention to the fact pattern and look for things that seem out of alignment with the spirit of the core values. Learn to trust those instincts.

After you answer, we'll provide guidance as to how specific core values apply to the fact pattern so that if you encounter these kinds of situations in real life you can think back to the hypothetical as a guide. Don't stress. If you answer incorrectly, it won't impact you negatively. Click next to go to the first hypothetical situation.

6.6 Hypothetical 1: Data Sharing Platform

6.7 Hypothetical 2: Exclusive Rights

6.8 Hypothetical 3: Proposition from Abroad

6.9 Hypothetical 4: Honorarium

6.10 Hypothetical 5: Cold Feet

6.11 University Resources

6.12 University Contacts

6.13 Certificate

Congratulations on reaching the end of this course. Type your name and then click the print button to print a copy of this certificate.

7. Section 3 - Additional Resources

7.1 Traveling Safely with Technology and Devices

Select a link to learn more about a topic or select close to return to where you left off.

7.2 Know Who You are Sharing With and What You are Sharing

Select a link to learn more about a topic or select close to return to where you left off.

7.3 U.S. Export and Sanctions Regulations

Select a link to learn more about a topic or select close to return to where you left off.

7.4 Protecting Information

Select a link to learn more about a topic or select close to return to where you left off.

7.5 Safety Regulations for Shipping Items and Materials

Select a link to learn more about a topic or select close to return to where you left off.

7.6 Collaboration

Select a link to learn more about a topic or select close to return to where you left off.

7.7 Authorship

Select a link to learn more about a topic or select close to return to where you left off.

7.8 Institutional Risk Management

Select a link to learn more about a topic or select close to return to where you left off.

7.9 Home Institution Resources for Collaborations

Select a link to learn more about a topic or select close to return to where you left off.

7.10 Malign Foreign Talent Recruitment Program

Select a link to learn more about a topic or select close to return to where you left off.

7.11 Federal Disclosure Requirements

Select a link to learn more about a topic or select close to return to where you left off.

7.12 Compliance With Regulatory Requirements

Select a link to learn more about a topic or select close to return to where you left off.

7.13 Protection of Institutional Resources

Select a link to learn more about a topic or select close to return to where you left off.

7.14 Reputational Risk

Select a link to learn more about a topic or select close to return to where you left off.

7.15 Institutional Considerations - Resources

Select a link to learn more about a topic or select close to return to where you left off.