Transcript

1. Course Introduction

1.1 Course Introduction

Welcome to research security training. This training 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. Select next to continue.

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 Router

Select section 1 to continue.

3. Section 1

3.1 Section 1: Introduction to Research Security

Section 1: Introduction to Research Security

3.2 Learning 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, the core values of academic research, and how undue foreign influence threatens the research community
- Recognize situations that may indicate undue foreign influence and that all stakeholders contribute to research security

3.3 Meet the Team

Vanessa

Hi! I'm Vanessa and I'm your guide for this training. Let's meet the team.

Fatima

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

Patrick

I'm Dr. Patrick H Davidson and I'm an associate professor.

Min-jun

I'm Dr. Park Min-jun and I'm an associate professor.

Rachel

I'm Rachel Painter and I'm a vice chancellor for research.

Emily

I'm Emily Green and I'm a research administrator.

3.4 Conference Introduction

Fatima

Hi Patrick and Min-jun! How's your week going?

Patrick

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. Would you like to join me?

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

Patrick

I'm looking at the conference app now. It says that international research collaboration is critical to advancing discovery and innovation and that research security is about safeguarding the research enterprise against the misappropriation of research and development.

Fatima

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

If researchers protect their pre-publication work, the U.S. will continue to inspire innovation, encourage investment in Research and Development and maintain a culture of trust and collaboration.

3.5 Keynote Introduction

The keynote speaker is about to define research security and how it is influenced by the federal landscape. The keynote address will provide a conceptual foundation for the U.S. approach to research security policy.

3.6 Keynote Introduction Video

One of my office's responsibilities in protecting research is to set policies and procedures to prevent the misuse of research funds.

3.7 Keynote Address

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 U.S. research ecosystem may seek to obtain ideas, inventions and investments through illicit means. This can impact researchers' careers.

3.8 Defining Research Security

So, what exactly is research security? Think of it as the collective system of controls that safeguards the research enterprise against the misappropriation of research.

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 include the set of regulations, policies, and procedures that protect the research enterprise from Intellectual Property theft, misuse, and unauthorized access.

3.9 Everyone Is Responsible

Every one of us shares responsibility for maintaining security. Our collective efforts help to 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.

3.10 Key Federal Regulations

To date, several key documents have been issued. Among them are:

- The JASON report Fundamental Research Security
- National Security Presidential Memorandum 33
- The Chips and Science Act

Click on each guidance document for more information. A link to each key document is included.

2019 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 conflicts of interest. It also recommends NSF and recipients investigate and adjudicate non-compliance.

2021 NSPM-33

National Security Presidential Memorandum 33 (NSPM-33). 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.

2022 CHIPS and Science Act

The CHIPS and Science Act boosts investments in Research and Development and mandates the NSF establish a research security and integrity information sharing and analysis organization for all stakeholders, develop a risk assessment framework, and provide research security training as a part of responsible and ethical conduct of research training. The Act defines malign foreign talent recruitment programs and directs agencies to prohibit membership in them.

3.11 Personal and National Benefits

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.

3.12 Core Values of Academic Research

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
- Research ethics

The core values that support these three principles are the topic of this interactive poster. They include:

- Openness and transparency
- Accountability and honesty

- Impartiality and objectivity
- Respect
- Freedom of inquiry
- Reciprocity
- Merit-based competition

Click on each of these core values for more information.

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. 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, 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 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 research 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.

3.13 Knowledge Check

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

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 identify 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?

Examples of information all covered individuals, also known as senior and key personnel, are asked to disclose are current and pending sources of research funding or in-kind support, outside employment, business ownership or a significant stake in a company, appointments, and affiliations.

How is Disclosed Information Used?

That’s a great question. Disclosed information can be used to properly assess an individual’s qualifications and capacity to perform the proposed and ongoing research and prevent overlap with other obligations. It can also be used to avoid duplication of research and assess potential conflicts of interest and commitment.

4.4 COI vs. COC

Fatima

Emily, 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.

Emily

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

What is a Conflict of Interest?

Let’s start with the formal definition of conflicts of interest, also referred to as a COI.

From NSPM-33, a conflict of interest refers to 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.

What is a Conflict of Commitment?

Sure. 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 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 one hundred percent 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.

4.5 Activities, Affiliations, and Support to be Disclosed

Fatima

Emily, can you tell me more about what needs to be disclosed?

Emily

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

This includes disclosure of certain in-kind resources like:

- Office or lab space
- Equipment
- Supplies
- Employees funded by external organizations

Now let's look at how that information is disclosed.

4.6 How to Disclose

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

The Common Form for Biographical Sketch

A biographical sketch requests identifying information on the researcher, and information on their professional preparation, appointments, positions, and products. The researcher must also certify the information provided is current, accurate and complete and that at the time of submission they are not a party to a malign foreign talent recruitment program. The common form for the biographical sketch and the table detailing what needs to be disclosed can be found here. NSF serves as the steward for these federal forms.

The Common Form for Current and Pending (Other) Funding

Current and pending support details the researcher's current and pending projects and proposals (including their sources of support), and information regarding any in-kind

contributions, such as office or laboratory space, equipment, supplies, and employee or student resources. The individual must also certify the information provided is current, accurate and complete and that at the time of submission they are not a party to a malign foreign talent recruitment program. The common form for current and pending (other) support and the table detailing what needs to be disclosed can be found here.

Institutional Outside Interest Disclosure

To identify and manage potential conflicts of interest or commitment, your home institution likely has policies requiring you to disclose any outside interests and activities that are related to your institutional expertise or responsibilities.

Examples of outside interests and activities that may need to be disclosed to your institution include, but are not limited to:

- Consulting engagements
- External appointments
- Intellectual property
- Ownership in an outside entity (such as stock, equity, options)
- Travel paid or reimbursed by a non-US entity

Check with your institution's conflict of interest policies or program staff for more information on its specific disclosure requirements.

4.7 Knowledge Check

What do I need to disclose? Select all that apply.

4.8 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.

4.9 Case Study

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, and 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 in restitution to NASA.

4.10 Section Wrap-Up

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 should discuss this with my colleagues.

4.11 Knowledge Check

Why are U.S. federal research agencies concerned about conflicts of interest, conflicts of commitment and problematic affiliations? Select all that apply.

4.12 Consequences Overview

In this section, learners will understand individual consequences and organizational consequences for failure to report completely and accurately. And finally, learners will understand the consequences of non-disclosure for the United States Research Enterprise.

4.13 Consequences

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. These include facing civil monetary penalties for intentional omission, they can face suspension and debarment, which would prevent them from participating in federal contracts or awards. 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?

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. Along with significant reputational risk and loss of intellectual property, organizations risk additional conditions and administrative consequences if material undisclosed information is identified. This includes risk of termination, pause, or withholding of funding. Financial penalties, loss of eligibility for future funding, and legal consequences.

Consequences to the U.S. Research Enterprise?

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 Learning Objectives

By the end of this training learners will be able to identify potential risks associated with international collaborative research and professional activities and strategies and resources to assess risks. 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. The goal of this training is to help you be aware of and understand how to manage potential risks of international collaborations and safeguard research. Let's begin with giving a talk internationally.

5.4 Scenario 1: Introduction

Doctor 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?

5.5 Scenario 1: Possible Risks

Select each button to learn about the potential risks of giving a talk internationally then select next to continue.

Traveling without required sponsor approval

Your sponsors may require prior approval before you travel abroad. Review the terms of your awards to identify and comply with all applicable travel pre approvals or restrictions. Consult your institution's policies regarding whether prior registration or approval of international travel is required and whether there are associated reporting requirements if part or all of your international travel will be paid for or reimbursed by a foreign individual, entity, or government.

Theft of Data

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 available at your institution, 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. Keep your device with you and physically secure. Use a secure internet connection and turn off WIFI 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. 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. Additional resources on traveling internationally with technology can be found here. Other risks to consider can be found here.

Sharing restricted or patentable information

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, obtain permission from your sponsor before sharing information. If your research is subject to non-disclosure agreements, ensure that your presentation, including question and answer sessions, does not disclose proprietary or confidential information. If your research is likely to result in an invention, it is important to disclose this through your technology transfer office prior to making a public presentation.

Violating U.S. export & 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

Beyond these research specific risks, it is unfortunate but true that international travel may involve infrequent but real threats to personal safety. Click here for travel and safety information from the Department of State, including country specific information.

5.6 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.

5.7 Scenario 2: Possible Risks

The academic culture is to share research results, data, and techniques broadly. It is important to consider that the sharing of unpublished findings has 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 intellectual property 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 of 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. Select each button to learn about potential risks of sharing data or materials and how to mitigate them, then select next to continue.

Providing resources to an organization or individual on U.S. restricted lists

There is a small but real risk that you could be sharing data or materials with an individual or institution on US government restricted lists. The United States 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 collaborator against US restricted and prohibited party lists prior to further engagement.

Safeguarding intellectual property and other protected information

To protect your intellectual property, including unpublished data and information, work with your institution to put data use or material transfer agreements in place before sharing data or materials to prevent loss of potentially valuable patent protections. 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. If you have registered IP rights in the U.S., these protections are territorial and do not extend automatically to foreign countries. Additionally, most countries are a "first to file" country for trademark registration and "first inventor to file" for patent registration and therefore grant registration to the first filer regardless of first use in the market. If IP is stolen in a foreign country, it can be difficult, if not impossible, to block its user for a patent registration. To protect IP, it is critical that investigators carefully manage access to all data. Non-public research findings that could be commercialized should not be discussed with anyone who is not a trusted colleague. In addition to these IP considerations, it is important to remember that data sharing should be consistent with your data management and sharing plan and participant consent if sharing data about human research participants. Other considerations include whether there could be potential for human rights abuse or military applications.

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 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 organization's export control official as needed.

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. Consult your organization's export control official as needed. Click here if you would like to learn more about Safety Regulations for Shipping Items and Materials.

5.8 Scenario 3: Introduction

Fatima is now planning a collaborative international research project. What does she need to consider?

5.9 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 I.P. protection. As your research collaboration ramps up and your team begins to produce results, there are things that the team should consider and discuss. When assessing potential collaborations it is important to understand who you are collaborating with and establish parameters. Select each button to learn more about the potential risks of collaborating on a research project, then select next.

Click here for questions to consider, many of which are derived from a 2019 JASON advisory group report, Fundamental Research Security, commissioned by the National Science Foundation.

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.
Click here if you would like to learn more about authorship.

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 and 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

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.

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.

5.10 Scenario 4: Introduction

Hosting international students and scholars. A postdoc 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 postdoc should work in Fatima's lab for six to twelve months.

5.11 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 collaborators could be on U.S. restricted lists

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.

Protect the host lab's intellectual property

Fatima must protect information and data for all projects and ensure that 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.

Ensure 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 security incidents should be reported to the security team immediately.

5.12 Scenario 4: Mitigation Strategies

As a routine security practice, Fatima provided her institution the necessary information for screening the visiting postdoc. Review sponsored research agreements for terms related to hosting visitors and obtain necessary approvals before commitments to host the student are made,if 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 internal risks.

5.13 Scenario 4: Cybersecurity Threats

Cybersecurity risks are another important consideration. Click each button to learn more.

Common Cybersecurity Threats

Be aware of the most common types of cybersecurity threats for researchers:

- **Phishing:** Where hackers send inquiries (for example, emails and text messages) to attempt to get you to divulge information
- **Malware:** Malicious software designed to damage systems
- **Social Engineering:** This involves deceiving or manipulating individuals to gain access to your data

These types of cybersecurity threats are often bundled together. You may receive an email or text message with a link that if clicked allows malware to be downloaded onto your device. Be aware and report this type of activity to your university.

Staying Safe Online

What can researchers do to stay safe online?

- **Go slow!** Do not be pressured to click links or move too quickly
- **Be suspicious.** Do not click a link if you are unsure of the sender
- **Verify.** When you receive a communication, verify it is legitimate before opening
- **Report.** Consult your university I.T. Security guidance if you believe you may have received a phishing attempt, downloaded malware, or been the victim of social engineering

Protecting Research Data

Tips for how to protect research data:

Password Security: Protect and regularly change your password. Do not use duplicate passwords for multiple accounts. If your password is ever compromised, it will give access to all of your accounts. Consider using a "passphrase" instead of a "password."

Mobile Security: Do not automatically click links that are emailed or texted to you. Be aware of malicious apps as well – only download from reliable sources. Secure your device with a lock screen to secure your data if your phone is lost or stolen. And enable encryption on your mobile device – look to activate this in your settings menu.

Avoid public WIFI: Hackers can see anything you send across unsecured networks.

Use your university VPN

Enable Multifactor Authentication

Install software updates on your devices

These tips will help you keep your electronic devices secure and protect your research data!

All security incidents should be reported to your institution's information security team immediately. Examples of security incidents include:

- Someone accessing your account
- If you replied to an unsolicited email that asked for institution specific information or other personal information
- A laptop containing unencrypted sensitive research data was lost

Any suspected or confirmed unauthorized access to a device should be reported to the Information Security and IT department.

5.14 Scenario 5: Introduction

One of Fatima's collaborators approaches her with an offer of an appointment at their foreign institution. Fatima is excited for the opportunity, but wants to make sure that she does not jeopardize her U.S. academic appointment or her funding from US government agency grants. She schedules time to meet with research administrator Emily Green to discuss what she needs to think about in making her decision.

5.15 Scenario 5: Possible Risks

Select each button to learn more about potential risks of accepting a foreign appointment and how to manage them, then select next to continue.

Participation 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 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. Click here for the latest federal definition of a foreign talent recruitment program.

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 . The Federal 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 federal research funding.

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 intellectual property, and overcommitment 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. You must fully understand the terms of any overseas appointment before you agree to them. Your institution may be able to assist you in determining whether your offer is coming from or consistent with such a program and whether the terms of the agreement violate integrity principles, institutional policies, other US laws and regulations or terms of award. Although most collaborations are mutually beneficial, researchers need to be aware of the reputational and legal risks of participating in a malign foreign talent recruitment program. The full definition of a malign foreign talent recruitment program can be found here and terms and examples can be found here.

Violating integrity principles, U.S. laws or regulations, or your institution's policies

Fatima seeks advice from her institution on whether the terms of the agreement constitute a malign program and violate integrity principles or U.S. laws or regulations and if not, what approvals might be needed to engage in the activity. Fatima will also make sure that accepting an offer is consistent with the policies of her home institution.

Violating terms of federal sponsor requirements

Conflicts can arise if the new appointment over-commits your effort compared to effort already committed on current sponsored projects, including committing to more research effort than there is time available or committing to do the same work for multiple sponsors. In addition, there may be agency prohibitions or prior approval requirements. Click here to learn more about federal reporting requirements, prior approvals, and resources.

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, Department of Energy, National Science Foundation and National Institutes of Health. Details can be found in individual agency guidance. Areas of commonality include concerns about engagement with entities and individuals on U.S. restricted list 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.

5.16 Scenario 5: Mitigation Strategies Animation

If you are offered an international appointment make sure that accepting that offer doesn't violate institutional and sponsor policies, especially policies on conflict of commitment before you sign the agreement. If there is a written agreement make sure you request and have reviewed a certified translation of the document before signing. If the agreement is subject to the 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 through an agreement negotiated by your institution , have your personal lawyer review all documents to ensure compliance with your current employment agreements and with US laws and regulations.

5.17 Scenario 5: Risk Mitigation

Which mitigation strategies are appropriate? Select all that apply.

6. Section 4

6.1 Section 4: International Collaboration

Section 4: International Collaboration

6.2 Introduction

Min-jun

I've learned a lot about research security today.

Fatima

Working across borders is absolutely crucial to global scientific progress. The goal is to be transparent and know when and how to get help from your colleagues, supervisors and

administrators. Shutting the door to international research and researchers would limit scientific discovery and innovation and impact health, the economy and security.

6.3 Core Values in the International Context

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.

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.

6.4 Hypothetical 1: Data Sharing Platform

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 core values of the U.S. research enterprise?

6.5 Hypothetical 2: Exclusive Rights

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?

6.6 Hypothetical 3: Proposition from Abroad

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?

6.7 Hypothetical 4: Honorarium

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?

6.8 Hypothetical 5: Cold Feet

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?

6.11 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. Lightbox Content

7.8 Foreign Talent Recruitment Program

Per the White House Office of Science and Technology Policy's February 2024 memo "A foreign talent recruitment program is any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue."

7.12 Internal Risks

An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. Insider threat involves the threat that an insider will use their authorized access, intentionally or unintentionally, to do harm to an organization's mission, resources, personnel, facilities, information, equipment, networks, or systems.

Insider threats can occur due to:

- **Negligence** – allowing someone to piggyback through a secure entry point, losing a laptop, or not updating antivirus or application software
- **Accident** – accidentally sending a sensitive email attachment or clicking a malicious link
- **Intent** – vengeance against another employee or the organization or stealing IP or unpublished research data for monetary or competitive advantage
- **Collusion** - Cooperating with an outsider to commit fraud, theft, or sabotage
- **Third-party threats** - Outsiders who obtain access to systems or data to commit fraud, theft, sabotage, or hold data ransom.