Research Security Training

Refresher Module

This abbreviated module satisfies federal research security training requirements for individuals who have previously completed the full NSF training module. Satisfactory completion of a quiz following the module is required to receive credit.

Authors

Allen DiPalma and Bill Yates

Office of Research Protections
University of Pittsburgh

REGULATORY REQUIREMENT

Section 10634 of the CHIPS and Science Act of 2022 codifies a research security training requirement for "covered individuals" on federally funded research and development awards. Commonly called "key personnel," a covered individual is someone who contributes in a substantive, meaningful way to the scientific development or execution of a federal research project and is designated as a covered individual by the relevant federal agency. The training must address cybersecurity, international collaboration, foreign interference, and rules governing the proper use of funds, disclosure, conflicts of commitment, and conflicts of interest.

Covered individuals must have completed research security training no more than 12 months before the submission of a new or competing research proposal, including new proposals, resubmissions, and competing grant renewals.

Both the covered individual and the University must certify the completion of this required training, subject to federal penalties for false certification.

Learning Objectives

Upon completion of this training module, participants will be able to:

- Define research security and identify the core values underlying the U.S. research enterprise.
- Describe the key federal reports, directives, and legislation governing research security, including the JASON Report, NSPM-33, and the CHIPS and Science Act.
- Identify what must be disclosed to federal funding agencies and the University, and distinguish between conflicts of interest and conflicts of commitment.
- Describe the individual and organizational consequences of non-disclosure.
- Identify a foreign component in a federally funded research study and describe the requirements for utilizing a foreign site.
- Define malign foreign talent recruitment programs, identify the prohibited terms, and explain the consequences of participation.
- Identify the primary U.S. export control and sanctions regimes and the comprehensively sanctioned countries.
- Apply best practices for mitigating research security risks during international travel, data sharing, and hosting of international visitors.
- Recognize common cybersecurity threats and apply basic protection measures.
- Articulate the shared responsibility for research security and the importance of informed, secure international collaboration.

1. What Is Research Security?

Research security is the collective system of controls that safeguards the research enterprise against the misappropriation of research and development. It encompasses the regulations, policies, and procedures designed to protect against the misappropriation of research findings, data, and intellectual property.

Core Values of Academic Research

The following core values underpin the U.S. research ecosystem. University of Pittsburgh scholars are expected to uphold the highest standards of integrity in their research, instruction, and evaluation activities. All research collaborations should adhere to these values.

Value	Description
Openness & Transparency	Making research data available for verification and reproducibility
Accountability & Honesty	Responsibility to taxpayers, Congress, students, and the research community
Impartiality & Objectivity	Conducting work without bias or external influence
Reciprocity	Even exchange of ideas and knowledge with mutual benefit to all parties
Merit-Based Competition	Fair, competitive evaluation of research based on intellectual value

Additional information about research integrity, research misconduct, and the University's related policies and procedures can be found on the University's Responsible Conduct of Research website.

> **KEY TAKEAWAY:** The goal of research security is not to limit international collaboration but to ensure that it is conducted on a foundation of transparency, integrity, and reciprocity.

2. Foundations for Research Security

The current federal research security framework has evolved through a series of reports, directives, and legislation issued between 2019 and 2022. Together, these establish the disclosure requirements, training obligations, and programmatic safeguards that govern federally funded research today.

2019

JASON Report on Fundamental Research Security

Commissioned by NSF, this independent advisory report affirmed the value of open fundamental research while emphasizing the need for full disclosure of commitments and potential conflicts of interest as a core element of research integrity.

2021

National Security Presidential Memorandum 33 (NSPM-33)

NSPM-33 established shared disclosure requirements across federal agencies, required the use of persistent digital identifiers, mandated research security programs at institutions receiving more than $50 million annually in federal research funding, outlined penalties for non-compliance, and encouraged information sharing across federal agencies to promote research integrity.

2022

CHIPS and Science Act

The CHIPS and Science Act codified research security training requirements for covered individuals, defined malign foreign talent recruitment programs (MFTRPs), and prohibited participation in such programs by individuals seeking or holding federal research awards.

3. Federal Agency Disclosure Requirements

Federal funding agencies, as well as the University, require disclosure to protect research integrity, ensure responsible stewardship of taxpayer funds, identify conflicts of interest and conflicts of commitment, and detect foreign government interference. The JASON Report established that full disclosure is a core element of research integrity. NSPM-33 and the CHIPS and Science Act built on that foundation by standardizing disclosure requirements across agencies and making them enforceable under law. Without disclosure, the safeguards designed to protect federally funded research cannot function.

This section outlines the disclosure obligations mandated by federal funding agencies. The University's separate disclosure requirements are addressed in the following section.

Conflict of Interest vs. Conflict of Commitment

Conflict of Interest (COI)	Conflict of Commitment (COC)
A financial interest or relationship that could affect the design, conduct, reporting, or funding of research	Conflicting obligations that compromise an individual's primary institutional duties, including situations where total effort commitments across all activities exceed 100% of available time

What Must Be Disclosed to Federal Agencies?

The following are required disclosure elements for most federal funding agencies. While these requirements are broadly consistent across agencies, some may require additional elements. Investigators should review each agency's specific application instructions to confirm the disclosure requirements that apply to their award.

Category	What to Disclose
Research Funding	All current and pending sources of research funding or in-kind support, whether domestic or foreign, regardless of whether directly related to the proposed project
Outside Employment	Outside employment, business ownership, or a significant financial stake in a company that relates to your institutional responsibilities
Appointments & Affiliations	All academic, professional, or institutional appointments and affiliations, whether paid or unpaid, domestic or foreign, full-time or part-time
In-Kind Support	In-kind contributions valued at $5,000 or more that require a time commitment, including equipment, materials, or services provided by external entities
Space & Resources	Office or laboratory space, equipment, supplies, or employees funded by external organizations that support your research activities
Startup Packages	Startup packages from entities other than the proposing organization, including those from foreign institutions
Foreign Programs	Participation in foreign government-sponsored programs, including talent recruitment programs, honorary appointments, and funded research positions abroad
Research Consulting	Consulting activities that involve the conduct of research, whether or not compensation is received

How are Disclosures Made to Federal Funding Agencies?

Most federal funding agencies have adopted standardized common forms to reduce administrative burden and promote consistency. These forms are prepared using SciENcv (Science Experts Network Curriculum Vitae), a web-based tool linked to each investigator's ORCID iD. Since not all federal agencies have adopted a common form, investigators should confirm the disclosure requirements for a federal agency before submitting a funding application.

Form	Description
Common Form for Biographical Sketch	Provides a standardized format for presenting an investigator's education, professional experience, publications, and relevant expertise. It allows reviewers to evaluate the research team's qualifications.
Common Form for Current and Pending (Other) Support	Requires investigators to disclose all sources of support — domestic and foreign, whether funded, pending, or in-kind — regardless of whether they are directly related to the proposed project. This form is critical for identifying potential overlaps in effort, conflicts of commitment, and undisclosed foreign support.

What are the Potential Consequences of Non-Disclosure to Federal Agencies?

Individual Consequences

- Civil monetary penalties
- Suspension and debarment from federal contracts and awards
- Prohibition from participation in peer review, proposal submissions, or award applications
- Criminal prosecution in severe cases

Organizational Consequences

- Termination, pause, or withholding of funding
- Financial penalties and loss of eligibility for future federal funding
- Reputational damage and loss of intellectual property protections

4. Institutional Disclosure Requirements

The following provides an overview of the University's mandatory disclosers — those required to submit disclosures — and the information they must disclose. The University's disclosure process is detailed on this website.

WHO MUST DISCLOSE

The following categories of University personnel are designated as **mandatory disclosers**:

- All full-time faculty members
- Part-time or adjunct faculty designated by their supervisor
- Individuals independently responsible for the design, conduct, or reporting of research, including all postdoctoral trainees
- Administrators and staff required to disclose due to their job responsibilities
- Individuals in a position to make, direct, or materially influence University business decisions
- Individuals with significant input over the selection of outside vendors or service providers

WHAT MUST BE DISCLOSED

Under University Policy RI 01, mandatory disclosers must disclose all financial, personal, and professional interests, activities, and relationships with non-University entities that create, or could be perceived to create, a conflict of interest or commitment that:

- ✓ Might reasonably be perceived to be related to the individual's institutional responsibilities
- ✓ Relates to the University's educational, research, service, or other missions, including the services offered by the University
- ✓ May otherwise present a conflict of interest or conflict of commitment, or the perception of such a conflict, with the individual's duties to the University

KEY DEADLINES

April 15	Annual conflict of interest disclosure due for all mandatory disclosers, even if they have no outside interests, activities, or relationships to disclose
June 15	Supervisor reviews of annual disclosures due
Within 30 days	New employees designated as mandatory disclosers must complete their initial disclosure
Within 30 days	Existing disclosers must update their disclosure when new outside activities, interests, or relationships arise

HOW TO DISCLOSE

All institutional disclosures are submitted through **MyDisclosures**, the University's electronic disclosure system. MyDisclosures captures both financial interests and time commitments to outside organizations in a single platform, allowing personnel and their supervisors to easily report, track, and review outside activities.

5. Foreign Components of Federally Funded Research

Federal funding agencies require that all significant research activities performed outside the United States be identified, disclosed, and authorized. These activities are known as "foreign components." Failure to properly disclose and obtain authorization for a foreign component may result in the return of funds, termination of the award, or other enforcement actions.

> 📖 **DEFINITION**
>
> A **foreign component** is the performance of any significant scientific element or segment of a project outside of the United States, either by the recipient or by a researcher employed by a foreign organization, whether or not grant funds are expended
>
> *This definition applies regardless of the funding source — NIH, NSF, DOE, DOD, and other federal agencies all require disclosure and authorization of foreign components, though specific procedures may vary by agency*

What Constitutes a Foreign Component?

The determination of whether an activity rises to the level of a foreign component depends on whether a "significant scientific element or segment" of the project will be performed outside the United States. The following examples illustrate the distinction.

✓ Likely a Foreign Component	✗ Typically NOT a Foreign Component
Collaborations with investigators at a foreign site anticipated to result in co-authorship	Foreign travel exclusively for consultation or conference attendance
Use of facilities or instrumentation at a foreign site for data collection or analysis integral to the project	Procurement of routine goods or services from a foreign vendor (e.g., custom synthesis of a small molecule, sample analysis)
Involvement of human subjects or vertebrate animals at a foreign site	Conference grant support for travel exclusively for attendance
Extensive foreign travel by project staff for data collection, surveying, sampling, or similar research activities	A researcher with foreign support when all grant-related research is conducted in the United States *(although this must be reported as Other Support)*
Receipt of financial support or resources from a foreign entity for the project	A foreign-born researcher working on the project entirely within the United States
Any activity of the recipient that may have an impact on U.S. foreign policy through involvement in the affairs or environment of a foreign country	Purchasing equipment or supplies manufactured abroad through a domestic distributor

How Foreign Components Must Be Authorized

The authorization process depends on when the foreign component is identified — at the time of the initial proposal or after an award has been made.

AT THE TIME OF PROPOSAL SUBMISSION

- All known foreign components must be disclosed in the proposal application
- A Foreign Justification document must be included, explaining why the work must be performed outside the U.S. and what unique resources, talent, or conditions the foreign site provides
- The application must identify the foreign country, the collaborating organization, and the nature of the activities to be performed abroad
- If selected for funding, approval of the foreign component is reflected in the Notice of Award

AFTER AN AWARD HAS BEEN MADE

Adding a foreign component to an existing award requires prior approval from the funding agency **before** the activity may begin. Investigators must:

1. Submit a prior approval request through the Office of Sponsored Programs (OSP) at least 30 days before the proposed change
2. Provide a description of the planned activities, a budget (if applicable), a timeline, and a Foreign Justification
3. Wait for written approval from the agency before initiating the foreign activity

A foreign component cannot be initiated prior to funding agency approval

Consequences of Non-Compliance

Failure to properly disclose and obtain authorization for a foreign component can have serious consequences for both the investigator and the institution:

- Return of funds or disallowance of costs associated with the unauthorized foreign activity
- Termination, suspension, or withholding of the award
- Audit findings and potential institutional sanctions
- Referral for investigation by the funding agency's Office of Inspector General
- In severe cases, debarment from future federal funding or criminal prosecution

6. Malign Foreign Talent Recruitment Programs (MFTRPs)

Participation in a malign foreign talent recruitment program renders an individual ineligible for federal research funding. This prohibition is established by the CHIPS and Science Act of 2022 and applies to all covered individuals on federally funded research awards.

What Is a Foreign Talent Recruitment Program?

Many countries encourage the growth of their research enterprise through programs designed to attract talented researchers. These programs often involve grants, fellowships, honorary titles, or other forms of compensation. Such programs are broadly referred to as foreign talent recruitment programs (FTRPs). Not all FTRPs are prohibited — routine international collaboration, scholarly presentations, and co-publication of fundamental research are generally permissible.

However, an FTRP becomes "malign" when it meets specific criteria defined in the CHIPS and Science Act.

WHEN IS A PROGRAM CONSIDERED "MALIGN"?

A foreign talent recruitment program is classified as malign when **both** of the following conditions are met:

1. **It is sponsored by a foreign country of concern**, or by an entity based in such a country — regardless of whether that entity is directly government-sponsored
   AND
2. **It includes one or more of the prohibited terms or conditions** listed below

Foreign Countries of Concern

Section 10638 of the CHIPS and Science Act defines the following as foreign countries of concern:

- People's Republic of China (including Hong Kong and Macau)
- Russian Federation
- Islamic Republic of Iran
- Democratic People's Republic of North Korea

Prohibited Terms and Conditions

A foreign talent recruitment program is malign if it is sponsored by a country or entity of concern and requires any of the following:

1	Unauthorized transfer of intellectual property, data, materials, or unpublished information
2	Recruitment of trainees or other researchers into the program
3	Establishment of a laboratory, research group, or position at a foreign institution
4	Inability to terminate the agreement except under extraordinary circumstances
5	Performance of work that creates overlap or duplication with a federal award
6	Application for funding from the sponsoring foreign government
7	Omission of acknowledgment of the U.S. institution or federal funding source
8	Non-disclosure of participation in the program
9	Any requirement that would otherwise violate the terms of a federal research award

✅ WHAT IS NOT CONSIDERED A MFTRP?

The following routine international activities are generally not considered foreign talent recruitment programs:

- Making scholarly presentations regarding scientific information not otherwise controlled under current law
- Participating in international conferences or other exchanges involving open and reciprocal sharing of scientific information
- Co-publishing fundamental research in peer-reviewed journals
- Receiving international research awards from organizations not on prohibited lists

However, if any of these activities are funded, organized, or managed by an entity on a restricted list, they may be classified as an FTRP and must be disclosed

Before Accepting a Foreign Appointment

If you are considering a foreign appointment, fellowship, or participation in any program sponsored by a foreign entity, take the following steps before signing any agreement:

☐ REQUIRED STEPS

- ✓ **Consult the Office of Research Security & Trade Compliance** (researchsecurity@pitt.edu) before signing any agreements — the office can assist in determining whether a program may be considered malign
- ✓ **Obtain a certified English translation** of all documents not in English before signing
- ✓ **Verify that the appointment does not overcommit your effort** beyond 100% of your available time when combined with your University obligations
- ✓ **Have a personal attorney review** any agreements entered into in a personal capacity
- ✓ **Report all foreign income to the IRS** as required by federal tax law
- ✓ **Disclose the appointment** in MyDisclosures and as required by funding agencies

Certification Requirements

Under the CHIPS and Science Act, both individuals and institutions must provide certifications regarding MFTRP participation:

Who	Certification Requirement
Covered Individuals	Must certify at the time of proposal submission — and annually thereafter for the duration of the award — that they are not a party to a malign foreign talent recruitment program
Institution	Must certify that each covered individual who is employed by the institution and listed on the application has been made aware of the MFTRP requirements

Fraudulent certifications or intentional omissions may result in criminal, civil, or administrative penalties.

💡 **TIP:** If you are unsure whether a foreign program, appointment, or agreement may constitute a malign foreign talent recruitment program, contact the Office of Research Security & Trade Compliance (researchsecurity@pitt.edu) before making any commitments. It is always better to ask first.

7. Export Controls & Sanctions

U.S. export control laws regulate the transfer of certain information, technologies, materials, and commodities to foreign countries and foreign nationals — including transfers that occur within the United States (known as "deemed exports"). These laws also restrict transactions with specific individuals, entities, and countries. Several federal agencies maintain restricted party lists identifying individuals and entities with whom U.S. persons are prohibited or limited from doing business. Failure to comply with export control laws can result in severe civil and criminal penalties for both individuals and the University.

📧 **NEED HELP?** The Office of Research Security & Trade Compliance (researchsecurity@pitt.edu) can assist University members in determining whether an international engagement — including the export of materials, data, or technology — is subject to export control regulations, and whether a foreign entity or individual appears on a restricted party list

Key Regulations

Three federal agencies administer the primary export control and sanctions frameworks. Each governs different categories of items and activities:

Regulation	Agency	What It Covers
ITAR	Department of State	International Traffic in Arms Regulations — governs defense-related articles, services, and technical data listed on the U.S. Munitions List
EAR	Department of Commerce	Export Administration Regulations — governs "dual-use" items with both commercial and potential military or intelligence applications, listed on the Commerce Control List
OFAC	Department of the Treasury	Office of Foreign Assets Control — administers economic and trade sanctions programs that restrict transactions with specific countries, entities, and individuals

📖 WHAT IS A "DEEMED EXPORT"?

A deemed export occurs when controlled technology, software, or technical data is released or disclosed to a foreign national inside the United States. This can happen through conversations, demonstrations, lab access, email, or shared documents. A deemed export can occur simply by allowing a foreign national access to controlled equipment or data in a research lab. The same license requirements that apply to a physical export are also applicable to the release of controlled technology to a foreign national on campus.

Comprehensively Sanctioned Countries

🚨 HIGHEST RESTRICTION

Cuba, Iran, and North Korea are subject to comprehensive U.S. sanctions. Most activities involving these countries — including financial transactions, provision of services, and transfer of goods or technology — require prior U.S. government authorization.

Additional significant restrictions apply to **Russia, Belarus, and the Crimea, Donetsk, and Luhansk regions of Ukraine.** Sanctions imposed by the U.S. government change over time; consult the Research Security and Trade Compliance website for current information.

⚠ It is particularly important to contact the Office of Research Security & Trade Compliance (researchsecurity@pitt.edu) prior to any engagement with individuals or entities in comprehensively sanctioned countries. This includes conference participation, data sharing, site visits, and collaborative research.

Consequences of Non-Compliance

Violations of export control laws and sanctions regulations carry severe penalties for both individuals and the University. Penalties vary by regulatory framework but can include:

Individual Consequences	Institutional Consequences
• Criminal fines up to $1,000,000 per violation • Imprisonment up to 20 years per violation • Civil penalties up to $1,270,000 or more per violation • Loss of export privileges	• Criminal fines up to $1,000,000 or more per violation • Debarment from government contracts • Seizure and forfeiture of goods • Reputational damage and loss of research partnerships

8. Risk Mitigation for International Activities

International research activities — including travel, data sharing, and hosting foreign visitors — require advance planning to ensure compliance with federal regulations, award terms, and University policies. Before engaging in international activities, researchers should consult the Pitt Global Operations website (globaloperations.pitt.edu) and the Office of Research Security & Trade Compliance website (researchsecurity.pitt.edu) for applicable guidance.

International Professional Travel

BEFORE YOU GO

- ✓ **Review your award terms and conditions** to determine if sponsor pre-approval for international travel is required. Some agencies require prior written authorization before any foreign travel on a funded award.
- ✓ **Register your trip** through the International SOS MyTrips portal, the University's official travel registry. Trip registration is required for all students and staff and strongly encouraged for faculty.
- ✓ **Verify export control requirements** before traveling with technology, data, or equipment. Some items may be prohibited or require an export license for certain destinations. The Office of Research Security & Trade Compliance (researchsecurity@pitt.edu) can assist with this determination.
- ✓ **Consider requesting a travel device** from the University's Global Operations Support rather than taking your personal or University-issued device. Loaner devices are available for faculty and staff.

WHILE TRAVELING

- ✓ **Use clean or encrypted devices;** carry only the data essential to the trip
- ✓ **Use a VPN** for all internet connections; avoid public Wi-Fi networks
- ✓ **Do not use foreign-provided USB drives** or connect to unknown devices
- ✓ **Use new, unique passwords** for accounts accessed during travel; change them again upon return
- ✓ **Keep devices physically secure** and in your possession at all times
- ✓ **Minimize access to sensitive accounts;** limit the websites and services you log into while abroad

WHEN YOU RETURN

- ✓ **Treat all devices used abroad as potentially compromised** – the safest course is to have the device securely erased and rebuilt
- ✓ **Change your University Computing Account password** and passwords for all services accessed while traveling
- ✓ **Report any suspicious activity** to Pitt Digital (412-624-HELP) or the IT Help Desk immediately

Sharing Data or Materials Internationally

Transferring research data, materials, or other items to a foreign collaborator requires careful attention to both regulatory requirements and award terms. The following steps should be completed before any international transfer:

📤 REQUIRED STEPS

- ✓ **Screen collaborators against U.S. restricted party lists.** The Office of Research Security & Trade Compliance can perform this screening on your behalf.
- ✓ **Execute a data use agreement or material transfer agreement** through the Office of Sponsored Programs before sharing any research data or materials with a foreign party.
- ✓ **Verify whether an export license is required** through the Office of Research Security & Trade Compliance (researchsecurity@pitt.edu). Some data, technology, and materials require prior government authorization before they can be shared with foreign nationals or sent abroad.
- ✓ **Check destination country import requirements.** Some countries have their own restrictions on the import of biological materials, chemicals, or technology.
- ✓ **Confirm that the transfer is permitted under your award terms.** Some funding agencies restrict or prohibit the sharing of data or materials with entities in certain countries.

Hosting International Visitors

The University's Academic Visitor webpage outlines the steps required to host visitors, including foreign visitors. In addition to completing the visitor process, hosts should take the following steps to protect research security:

👥 HOST RESPONSIBILITIES

- ✓ **Protect host laboratory intellectual property.** Educate all lab members on security expectations and what information may and may not be shared with the visitor.
- ✓ **Limit the visitor's access to information** necessary for the specific collaboration. Do not provide broad access to lab data, systems, or equipment beyond what the collaboration requires.
- ✓ **Confirm that any transmission of data or information to the visitor is permitted** by the funding agency supporting the research. Some awards restrict the involvement of foreign nationals or the sharing of data with individuals from specific countries.
- ✓ **Be aware of deemed export rules.** Providing a foreign national with access to controlled technology or technical data in your lab may constitute a deemed export and could require a license.

💡 **TIP:** When planning any international activity — whether travel, data sharing, or hosting a visitor — start the compliance review process early. Restricted party screenings, export license determinations, and data use agreements all take time to complete. Last-minute requests can delay your research.

9. Cybersecurity Best Practices

Cybersecurity threats target the most vulnerable point in any organization's security infrastructure: its people. Understanding common threats and practicing basic cybersecurity hygiene are essential to protecting both your research and the University.

Common Threats

The following are among the most frequent cybersecurity threats encountered in research environments:

Phishing

Deceptive emails, text messages, or websites designed to trick you into revealing sensitive information such as login credentials, financial data, or personal information

Malware

Malicious software — including viruses, ransomware, spyware, and trojans — designed to damage systems, steal data, encrypt files for ransom, or gain unauthorized access to your computer or network

Social Engineering

Manipulating individuals through psychological tactics — such as impersonation, pretexting, or building false trust — to gain access to sensitive information or systems

Protection Measures

The following practices significantly reduce your risk of falling victim to a cyberattack.

ESSENTIAL CYBERSECURITY HABITS

- ✓ **Do not click suspicious links.** Verify the sender's identity before responding to unexpected emails or messages. Hover over links to check the actual URL before clicking. When in doubt, contact the sender through a known, separate channel.
- ✓ **Use strong, unique passwords.** Use a different password for each account. Consider passphrases — a string of random words — for added security.
- ✓ **Enable multi-factor authentication (MFA)** on all accounts that support it. MFA requires a second form of verification beyond your password, making it significantly harder for attackers to access your accounts even if your password is compromised.
- ✓ **Install software updates promptly.** Security patches fix known vulnerabilities that attackers actively exploit. Enable automatic updates where possible for your operating system, applications, and web browsers.
- ✓ **Use the University VPN** when accessing University resources remotely. Avoid public Wi-Fi networks for any work involving sensitive data.
- ✓ **Report all security incidents immediately.** If you suspect your account has been compromised, you receive a suspicious message, or you notice unusual activity, contact the Pitt Digital Help Desk at 412-624-HELP (4357) or helpdesk@pitt.edu. The Help Desk is available 24/7.

TIP: Pitt Digital provides comprehensive information on security standards and best practices.

10. Key Takeaways

1. **Disclose fully and accurately** — all funding sources, affiliations, and support must be reported.
2. **Know the regulations** — NSPM-33, the CHIPS and Science Act, and agency-specific requirements govern your obligations.
3. **Assess collaboration risks** — screen parties, protect intellectual property, and verify the terms of all agreements.
4. **Avoid MFTRPs** — review all foreign offers carefully. Participation renders individuals ineligible for federal research funding.
5. **Practice good cybersecurity** — protect devices, data, and credentials at all times.
6. **Consult your institution** — before international travel, sharing materials, or accepting foreign appointments.
7. **International collaboration is vital** — the goal is informed, secure engagement, not the avoidance of international partnerships.

Everyone shares responsibility for research security