Research Security Overview and Actions

Research&Innovation

Research Security Landscape - What to Expect

Since 2019, the federal government has imposed a series of research security-based regulations. These regulations continue to evolve and will include new and expanded regulations. Cornell is partnering with researchers to ensure that all activities are conducted compliantly.

- **Malign Foreign Talent Programs**: Largely prohibited.
- **Disclosures:** Complete and accurate disclosures of all outside activities (paid and unpaid), in-kind and other support, and foreign travel are of the utmost important.
- **Foreign Countries of Concern:** All engagements with individuals or entities in China, Russia, Iran, or North Korea must be reviewed by the research security office.
- **Cybersecurity**: We are expecting new federal requirements impacting the security of devices used on awards.*
- **Foreign Travel**: We are expecting new federal requirements that some or all foreign travel be pre-approved.*
- **Export Control**: Per usual, all international shipments and use of controlled technology at Cornell must be pre-approved by Cornell's Export Control Office.
- **Training**: Numerous new federal mandates for training. In order to meet these requirements, all researchers will be required to take Cornell's new Research Security and Responsible Conduct of Research Course. This course will be assigned through Culearn, before the end of 2023.

***Watch for additional communication as we learn more**

What is Driving These Changes?

Evolving Regulations – Specific Federal Requirements

NSPM-33 – What Do You Need to Know?

<u>Rest assured</u>, Cornell is well positioned to address the requirements and is looking forwarding to partnering with researchers to ensure all obligations are met.

- **What is it?**
  - NSPM-33 (National Security Presidential Memorandum-33) is a directive to all federal agencies to implement certain requirements for U.S. Government-supported research.
  - As a result, all federal agencies are in the process of implementing new security requirements, which Cornell (and all researchers) will be required to comply with.
- **What kind of security requirements?** Cornell is required to establish a research security program that includes the following areas:
  - **Cybersecurity**: Basic safeguards and protocols must be established on all devices used in the performance of a federal award
  - **Foreign Travel Security**: We are anticipating that, in the near future, some or all international travel, will need to be pre-approved.
  - **Research Security and Export Control Training**: All researchers must receive training in these areas.

NSPM-33 – What Do You Need to Know?

- **Continued Focus on Proper Disclosures:**
  - Generally, sponsors want to know about:
    - All outside appointments and employment (whether paid or unpaid);
    - Subsidized travel from a foreign entity;
    - Current and Pending/Other support disclosures
      - Support to individuals (i.e., a visiting scholar paid by another entity)
      - International collaborations, even when no money is exchanged
      - Current and pending support/proposals
      - In kind contributions (even those not intended for use on the project)
- **Where can I get sponsor-specific information about what I should be disclosing?**:
  - NSF PAPPG
  - NIH Other Support
  - NIH Biosketch
  - NIH Foreign Components

- **Cornell's webpage on disclosure support**

CHIPS and Science: What Do You Need to Know?

- **Why do we need to care about the CHIPS and Science Act?**
  - The CHIPS act, like NSPM-33, directs agencies to require institutions like Cornell, to implement research security measures.
  - These measures may apply, **regardless of whether you receive CHIPS funding**.
  - Certain requirements apply to all federally funded researchers.

CHIPS and Science: Talent Programs

- **Malign Foreign Talent Recruitment Programs** (MFTRPs):
  - **Individuals:** Everyone listed in a proposal must certify that they are not a party to an MFTRP in the proposal submission and annually afterwards for the duration of the award.
  - **Institutions:** Each proposing organization must certify that each covered individual who is employed by such institution of higher education or other organization has been made aware of the requirements for MFTRPs and complied with the requirement.

***The purpose of the MFTRP prohibition is to ensure that the U.S. retains its top scientists, and that our research is protected from improper foreign government interference.**

CHIPS and Science: Malign Foreign Talent Recruitment Programs (MFTRPs)

An MFTRP is defined as any type of program, position or activity that involves one of more of the following:

- Unauthorized transfer of intellectual property, materials, data or other nonpublic information;
- Recruitment of trainees or researchers to enroll in such program, position or activity;
- Establishing a laboratory or entity in a foreign country in violation of terms and conditions of a federal research award;
- Accepting a faculty position, or undertaking any other employment or appointment in violation of the standard terms and conditions of a federal research award;
- Being unable to terminate the activity except in extraordinary circumstances;
- Being limited in capacity to carry out a federal research award;
- Requirement to engage in work that overlaps or duplicates a federal research award;
- Requirement to obtain research funding from the foreign government's entities;
- Requirement to omit acknowledgement of the U.S. home institution and/or the federal funding agency;
- Requirement to not disclose participation in the program, position, or activity; **OR**
- Having a conflict of interest or commitment contrary to a federal research award.

AND….

CHIPS and Science: Malign Foreign Talent Recruitment Programs (MFTRPs)

….AND

Is sponsored by one of the following:

- A foreign country of concern*; or
- An entity based in a foreign country of concern; or
- An institution or program on a restricted list .

*defined as the People’s Republic of China (includes Hong Kong and Macao), the Democratic People's Republic of Korea, the Russian Federation, the Islamic Republic of Iran, or any other country determined to be a country of concern by the Secretary of State;

CHIPS and Science: National Security Guardrails

- **What are these national security guardrails?** Recipients of CHIPS incentive funds are federally required to comply with certain requirements when engaging with “foreign entities of concern.”

- **What does this mean for Cornell?** This is an evolving issue and one we are watching closely. For now, all collaborations with entities or individuals located in China, Russia, Iran, and North Korea must be reviewed by the research security office.

DoD Policy: Countering Unwanted Foreign Influence in Fundamental Research

- **Is this new?** Yes, DoD just released a new policy telling us how they will be reviewing and assessing fundamental research projects.

- **Why?** In accordance with NSPM-33 and the new federal research requirements, DoD wants to "ensure security of DoD funded fundamental research, ensure that individuals fully disclose all information, and provide clear messaging on acceptable and encouraged behavior, as well as activities that may lead to challenges in securing DoD funding."
- **Tell me more about these security reviews?**
  - Security reviews will be conducted, at a minimum, on all fundamental research project proposals that are selected for award based on technical merit.
  - DoD is instructed to use publicly available information to validate information disclosed by individuals.
  - DoD will conduct periodic spot checks of individuals on DoD awards.
  - Security reviews must not discourage international research collaboration or impact time to award if possible.

DoD Policy: Strategies to Mitigate Risk

- **What if DoD identifies something that they don't like?**
  - DoD may require individuals or the institution to do some of the following, to mitigate identified risks:
    - Complete inside risk awareness training;
    - Increase frequency of reporting through RPPR;
    - Replace individuals on projects with other, lower-risk, individuals;
    - Provide copies of external contracts; or
    - Resign from positions deemed problematic by the risk-based security review.

DoD Policy: Risk Matrix

- **What has DoD identified as a potential problem?**
- **Prohibited factors**:
  - As of August 9, 2024, DoD is prohibited from providing funding to or making an award in which someone on the award is participating in a MFTRP, or to a proposing institution that does not have a policy addressing malign foreign talent programs.

- **Factors requiring mitigation (proposal will be rejected if mitigation is not possible):**
  - Indications that you are participating in a FTRP (no malign requirement).
  - Indications that you are currently receiving funding from a Foreign Country of Concern (FCOC) or a FCOC-connected entity.
  - Patents or patent applications that resulted from USG funded research, that were filed in an FCOC prior to filing in the U.S. or filed on behalf of an FCOC connected entity.
  - Indication of association with an entity on a U.S. restricted party list.

***Denial of award should only occur if mitigation is impossible; denials must be explained, and institutions may challenge a denial.**

DoD Policy: Risk Matrix

- **Mitigation measures will be recommended:**
  - Indications that someone on the award received funding from a FCOC or an FCOC-connected entity.

- **Mitigation measures suggested:**
  - Indications that your co-authors are participants in a FTRP (malign or otherwise).
  - Indications that you received limited or partial funding from an FCOC or an FCOC-connected entity.
  - Patents or patent applications that resulted from USG funded research, that were filed in a non-FCOC prior to filing in the U.S. or filed on behalf of a non-FCOC connected entity.
  - Co-patent application with someone on a U.S. restricted party list.
  - Indications that your co-authors are affiliated with an entity on a U.S. restricted party list.

NIH Foreign Subaward Requirements

NIH has issued the "NIH Updated Policy Guidance for Subaward/Consortium Written Agreements"

- **What does this mean for my NIH proposals and awards?**
  - NIH will require Cornell to ask potential subrecipients, at the application stage, to submit language in their letters of support indicating the subrecipient's willingness to abide by all requirements.
  - All subrecipients must enter into a formal agreement that addresses the scientific, administrative, financial, and reporting requirements of the grant.
  - If a subrecipient is unwilling to accept the requirements, then the award cannot be issued.

- **What is the "foreign" part about?**
  - For foreign subrecipients, the agreement must include a provision that the foreign subrecipient will provide access to copies of **all lab notebooks, all data, and all documentation that supports the research outcomes** as described in the progress report, to the primary recipient with a frequency of no less than once per year. Such access may be entirely electronic.

NIH Foreign Subaward Requirements

- **What about basic procurements from a foreign vendor?**
  - These requirements do not apply to vendors that are providing routine goods and services within normal business operations that are ancillary to the operation of the research program. The vendor must also be providing similar goods and services to many different purchasers and provide them in a competitive environment.

- **When does this requirement go into effect?**
  - January 1, 2024

New Rules for TikTok

- **Does this apply to me?** Right now, this applies on a contract-by-contract basis. If it is in your award, the PI will be notified and will be reaching out. **If it's not in your award, it doesn't apply.**

- **What is it?** New federal regulations prohibits TikTok or any product or app made by ByteDance Limited being **installed** on **any device** used in the performance of certain federal awards.

- **What devices are covered**? Any device, whether personally owned or Cornell owned, including cell phones and computers. The requirement applies to any device use to perform even simple activities such as making phone calls or answering emails related to the federal award.

- **How are we complying?** As an immediate measure, PIs on impacted awards will be asked by their GCO to sign an attestation stating that they have communicated to the requirement to everyone working on the award, under their direction.

How Research & Innovation Partners with Researchers to Address Federal Requirements

Research&Innovation

Cornell Actions

What is Cornell doing to prepare?

- Cornell is actively monitoring the regulations, talking to our peers, and engaging with professional associations.
- We are engaging in cross collaboration (OVPIA, OVPRI, OSP, CTL, ORIA…)
- We have created a new research security webpage and will be keeping it updated.
- We will address policy requirements in Cornell policies as required (ex: MFTRPs).
- Conflict of Interest disclosures may look a little different.
- We screen entities against restricted party lists.
- Alerts from RASS for sponsored projects involving entitles located in foreign countries of concern.

Cornell Actions

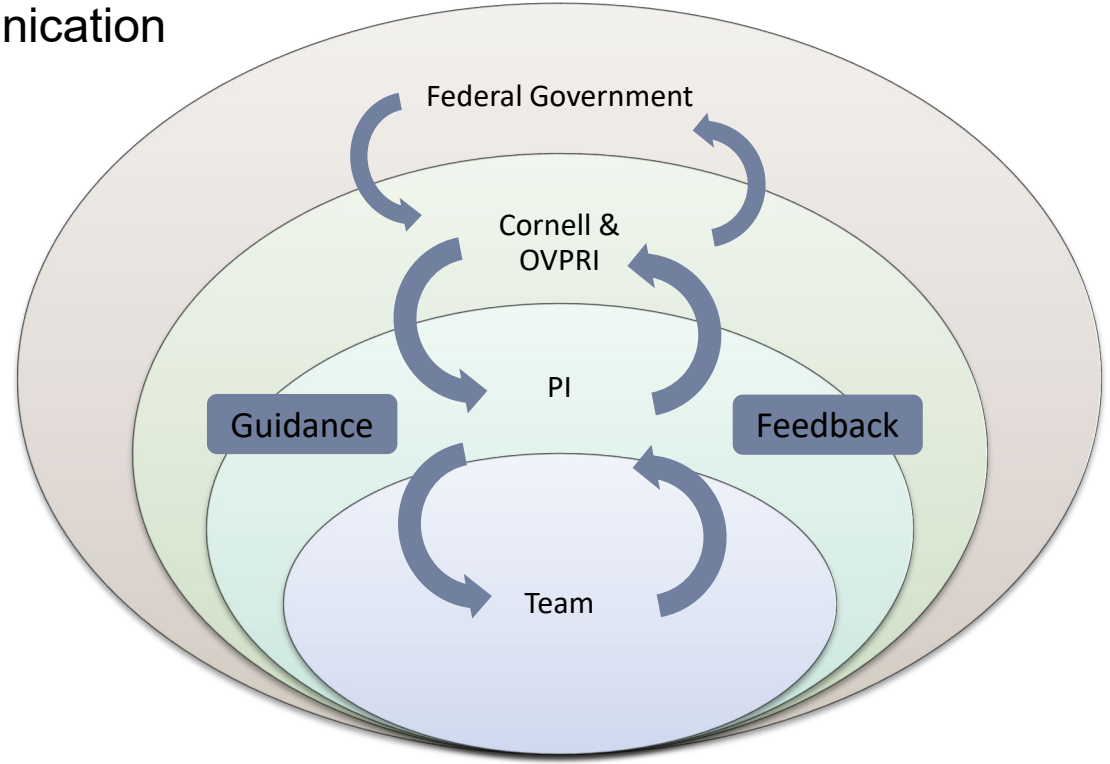
- Cornell is waiting for the federal government to release the final requirements for research security programs.
- Once released, we will partner with you to ensure that researchers and Cornell as an institution are following the federal mandates.
- We are anticipating the following:
  - Some or all foreign travel will require prior approvals
  - Some projects will require cybersecurity attestations
- Cornell has created an online course which will be released soon through CULearn. Our intention is that this course will assist researchers in meeting the federally mandated training requirements.
  - 30 minutes of video with supplementary reading materials
  - Requirement for everyone engaged in research
  - This simple course will fulfill all training requirements currently contemplated.

What do researchers need to do?

- Ensure that your COI report in Cornell's system is accurate, complete, and up to date.
- Ensure that all federal disclosures and reports are accurate, complete, and up to date.
- Ensure that information entered in RASS for your sponsored projects is accurate and complete.
- Take the CULearn training when it is assigned.
- Contact the research security office if you are contemplating entering into a collaboration with an entity in China, Russia, Iran, or North Korea.
- Reach out to the export control office prior to shipping anything internationally or engaging with restricted technology.
- Watch for additional communications.
- Reach out with questions.

How is messaging happening?

- Share feedback
- Collaboration and communication



Where can researchers get help?

- **Where can I learn more about Cornell's research security program**
  - Check out our website: https://researchservices.cornell.edu/research-security
  - Contact: researchsecurity@cornell.edu
- **How do I know if my co-author is a restricted party?**
  - Cornell's export control office can screen any entity. Please contact exportcontrols@cornell.edu
- **How do I know if I'm participating in a MFTRP?**
  - Reach out to researchsecurity@cornell.edu or review our website: https://researchservices.cornell.edu/resources/malign-foreign-government-talent-recruitment-programs
- **Who can I contact for help with the NIH foreign subaward requirements?**
  - Contact your Grant and Contract Officer in the Office of Sponsored Programs

Brief Recap

Research Security: Brief Recap

- **Malign Foreign Talent Programs**: Largely prohibited. Please reach out if you suspect you may be participating in one.
- **Disclosures:** Complete and accurate disclosures of all outside activities (paid and unpaid), in-kind and other support, and foreign travel are of the utmost important. When in doubt, disclose.
- **Foreign Countries of Concern:** All engagements with individuals or entities in China, Russia, Iran, or North Korea must be reviewed by the research security office.
- **Cybersecurity**: Expect new requirements impacting the security of devices used on awards.*
- **Foreign Travel**: Expect new federal requirements that some or all foreign travel be pre-approved.*
- **Export Control**: Per usual, all international shipments and use of controlled technology at Cornell must be pre-approved by Cornell's Export Control Office.
- **Training**: In order to meet the federal mandates for training, all researchers will be required to take Cornell's new Research Security and Responsible Conduct of Research Course. This course will be assigned through Culearn, before the end of 2023.

***Watch for additional communication as we learn more**

Contact

Office of Research Integrity and Assurance - Research Security:

Website: https://researchservices.cornell.edu/research-security

General Email: researchsecurity@cornell.edu

Research Security POC: Sarah Schlagter, Director of Research Integrity and Security

- sms655@cornell.edu
- 607-255-5284

Thank You