Research Security Compliance Updates

Research&Innovation

NSPM-33 Overview

National Security Presidential Memorandum (NSPM) -33

NSPM-33: Background

- **January 2021: NSPM-33:** "directs action to strengthen protections of United States Government-supported Research and Development (R&D) against foreign government interference and exploitation."

- Specifically, directs agencies to:
  - Require disclosures that enable reliable determinations where conflicts of interest and commitment exist.
  - Ensure that the organizations have established policies and processes to identify and manage risks to research security and integrity.
  - Ensure the availability and application of effective consequences for violations of disclosure policies and for engagement in other activities that threaten the security and integrity of the United States R&D enterprise

- Directs the Director of the Office of Science and Technology Policy (OSTP), through the National Science and Technology Council (NSTC), to coordinate activities to protect federally funded R&D from foreign government interference.

NSPM-33: Background

- **January 2022**: National Science and Technology Council (NSTC) releases guidance to federal departments and agencies regarding implementation of NSPM-33.

- Specifically, it includes general guidance for agencies, followed by more detailed guidance in **five key areas:**
  - Disclosure Requirements and Standardization
  - Digital Persistent Identifiers
  - Consequences for Violation of Disclosure Requirements
  - Information Sharing
  - Research Security Programs - Provide clarity regarding research security program requirements, how research organizations will be expected to satisfy the requirement, and how agencies will contribute to program content development

NSPM-33: Research Security Program Final Rule

- **July 2024**: OSTP Releases Guidelines for Research Security Programs at Covered Institutions

  - **Cybersecurity -** institution will implement a cybersecurity program consistent with the cybersecurity resource for research institutions described in the CHIPS and Science Act within one year after the National Institute of Standards and Technology (NIST) of the Department of Commerce publishes that resource

  - **Foreign Travel Security** – institution will implement periodic training on foreign travel security to covered individuals engaged in international travel, including sponsored international travel, for organization business, teaching, conference attendance, or research purposes AND implement a travel reporting program, to include an organizational record of international travel, including sponsored international travel, for organization business, teaching, conference attendance, and research purposes by covered individuals

NSPM-33: Research Security Program Final Rule

- **July 2024**: OSTP Releases Guidelines for Research Security Programs at Covered Institutions
  - **Research Security Training** – implement a research security training program by (A) certifying that (1) the institution requires covered individuals to complete training modules made available by the National Science Foundation (NSF) (or successor trainings developed by the federal government designed to satisfy the relevant requirements of the CHIPS and Science Act and NSPM-3322) and (2) each such covered individual has completed such trainings; or (B) certifying that the institution requires covered individuals to complete research security training and each such covered individual has completed the research security training program. The research security training program shall (1) provide covered individuals with explicit examples of behaviors that have resulted in a known improper or illegal transfer of U.S. government-supported R&D in the context of the research environment, as described to the covered institution by federal research agencies; and (2) communicate to covered individuals the importance of U.S. researcher participation in global discoveries, including attracting foreign talent to U.S. research institutions, as a core principle of maintaining international leadership and national security.
  - **Export Control Training** - certify that the institution requires covered individuals who perform R&D involving export-controlled technologies to complete training and that each such covered individual has completed training on complying with (1) U.S. export control and compliance requirements to relevant covered individuals; and (2) requirements and processes for reviewing foreign sponsors, collaborators, and partnerships.

CHIPS and Science Act Overview

Research Security Provisions

Research&Innovation

CHIPS and Science: About

- **August 2022:** CHIPS and Science Act of 2022 (H.R.4346) includes provisions for Research Security.
- **NSF Research Security:**
  - The Director of the NSF shall appoint a Chief of Research Security, whose primary responsibility shall be to manage the Research Security and Policy office.
  - The NSF shall develop an online resource that contains up-to-date information, tailored for institutions and individual researchers, including, among other things an explanation of NSF research security policies, and unclassified guidance on potential security risks that threaten research integrity and other risks to the research enterprise.
  - The Research Security and Policy office, in coordination with the NSF's Office of Inspector General, shall have the authority to conduct risk assessments of research and development award applications and disclosures to the NSF.
  - Requires training and oversight to be provided to postdoctoral researchers, faculty, and other senior personnel and requires the training and oversight to include (1) mentor and mentorship training; (2) training to raise awareness of potential research security threats; and (3) federal export control, disclosure, and reporting requirements.
  - The NSF must request annually from a recipient institution of higher education a disclosure of any current financial support that is $50,000 or more, including gifts and contracts, received directly or indirectly from a foreign source associated with a foreign country of concern.

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

- **Individuals:** Each federal research agency must require that each individual listed in a proposal 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 institution of higher education or other organization applying for such an award 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 listed above.

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: Malign Foreign Talent Recruitment Programs (MFTRPs)

Exceptions:

- The certifications do not apply retroactively to research and development awards made or applied for prior to the establishment of the policy by the Federal research agency.
- Federal agency policies shall not prohibit the following activities*** unless they are funded, organized, or managed by a prohibited party:
  - making scholarly presentations and publishing written materials regarding scientific information not otherwise controlled under current law;
  - participation in international conferences or other international exchanges, research projects or programs that involve open and reciprocal exchange of scientific information, and which are aimed at advancing international scientific understanding and not otherwise controlled under current law;
  - advising a foreign student enrolled at an institution of higher education or writing a recommendation for such a student, at such student's request; and
  - other international activities determined appropriate by the Federal research agency head or designee.

******More on this later***

CHIPS and Science: Training

- **Training Requirement:** Each individual listed on the application for an award must certify that they have completed within one year of such application, research security training, and each institution of higher education must certify that each individual who is employed by such institution and listed on the application has completed such training. Training must include:
  - Training to raise awareness of potential research security threats;
  - Federal export control;
  - COI disclosure and reporting requirements;
  - Intellectual property protection; and
  - Undue foreign influence.

DoD Policy on Countering Unwanted Foreign Influence in Fundamental Research

How DoD will Assess Fundamental Research Projects Going Forward

DoD Policy: Background

- **June 2023**: In accordance with NSPM-33,the Under Secretary of Defense for Research and Engineering signed this policy that requires all fundamental research projects that are selected for award by the DoD to go through a review for conflicts arising from foreign influence.

- **Goals:**
  - Ensure security of DoD funded fundamental research.
  - Ensure that individuals fully disclose all information.
  - Provide clear messaging on acceptable and encouraged behavior, as well as activities that may lead to challenges in securing DoD funding.

- Security reviews shall be conducted, at a minimum, on all fundamental research project proposals that are selected for review based on technical merit.
- DoD is instructed to use publicly available information to validate information disclosed by individuals.

DoD Policy: Strategies to Mitigate Risk

- DoD Components 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: Policies for Rejection

- When a decision not to make an award is based on research security risks, DoD must adhere to the following:
  - Leadership at DoD must have determined that one or more risks are unable to be mitigated, and that the risks are unacceptable.
  - Any rejection shall be explained in a risk-based security review rejection letter.
  - Upon rejection, a letter will be sent to the DoD Undersecretary for Defense, who will disseminate the letter to other DoD Components.

DoD Policy: Other Information

- DoD will conduct periodic spot checks of individuals on DoD awards.
- A decision matrix has been created to inform universities of risks that are unacceptable, and those that can be mitigated.
- DoD may adjust the risk matrix as needed, to incorporate changes in law and policy.

DoD Policy: Risk Matrix

- **Prohibited factors**:
  - As of August 9, 2024, DoD is prohibited from providing funding to or making an award in which a covered individual 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 a covered individual is participating in a FTRP (no malign requirement).
  - Indications that a covered individual is 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 (consider whether disclosed in proposal).
  - Indication of association with an entity on a restricted party list.

DoD Policy: Risk Matrix

- **Mitigation measures recommended:**
  - Indications that a covered individual received funding from a FCOC or an FCOC-connected entity.

- **Mitigation measures suggested:**
  - Indications that a covered individual's co-authors are participants in a FTRP (malign or otherwise).
  - Indications that a covered individual 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 (consider whether disclosed in proposal).
  - Co-patent application with someone on a restricted party list.
  - Indications that a covered individual's co-authors are affiliated with an entity on a restricted party list.

DoD Policy: Risk Matrix Notes

- **Covered Individual:** someone who contributes significantly to the design or execution of a project and who is considered essential to the successful performance of the project. Includes everyone listed as key personnel.

- **Foreign Country of Concern**: The People's Republic of China. The Democratic People's Republic of Korea, the Russian Federation, and the Islamic Republic of Iran.

- MFTRP definition in the DoD policy ***does not include*** the exceptions listed in the CHIPS and Science Act.

Cornell Status

NSPM-33: Cornell Status

Disclosure Requirements and Standardization:

Robust existing policies for Financial Conflict of Interest Related to Research and Conflicts of Interests and Commitment

RASS COI Disclosure System:

- Requires reporting of equity interests.
- Requires reporting of compensated travel.
- Additional questions include work at foreign locations, work with proprietary technology, and involvement of students.
- Required certification that “the outside activity has been or will be reported to federal and other sponsors in accordance with the sponsoring entity’s requirements.” Links to the website where they can find additional information.
- Includes notice of the Contract Addendum requirement.
- Ongoing updates – stay tuned

NSPM-33: Cornell Status

Research Security Program:

Cybersecurity

- ITSO 100: Cyber Security Awareness now required.
- Response procedures document in Policy 5.10.
- Per CIT we do comply with the enumerated requirements for institutional devices and equipment.

Foreign Travel Security

- Everyone is required (per Policy 8.5) to register their Cornell-related international travel plans to the Cornell International Travel Registry.
- As of November 1, 2024, international travel that is not preregistered will be classified as non-authorized and business-related travel expenses will not be reimbursed
- https://travelregistry.cornell.edu
- Cornell has a high-risk travel loaner device program.
- Cornell maintains a comprehensive International Incident Response Plan (IIRP). This plan is designed as a guide with protocols and procedures for responding to a situation abroad that affects our travelers.
- International Travel Advisory and Response Team (ITART): A group of senior-level administrators who meets regularly to discuss travel policies and ongoing situations abroad. They are on standby to convene and respond in the event of an emergency. ITART reviews high-risk travel petitions.

NSPM-33: Cornell Status

Research Security Program:

Research Security Training:

- CU601 Training includes research security, foreign interference, export control, conflicts, international travel, and research misconduct.

Export Control Training:

- The Export Control Office (ECO) provides departmental specific training.
- Anyone working with controlled technology must receive training from the ECO.
- Cornell subscribes to the Citi Course Export Control Module.
- All Grant and Contract Officers in OSP receive Export Control training.
- Export Control is one of the modules in Cornell's Research Administration Certification Program which takes place twice per year.

CHIPS and Science: Cornell Status

Research Security Training:

- Similar to NSPM-33 requirement.
- CU601

Malign Foreign Talent Recruitment Programs:

- Website: https://researchservices.cornell.edu/resources/malign-foreign-government-talent-recruitment-programs
  - "Participation in a Malign Foreign Government Talent Recruitment Program by any Cornell employee or researcher, is strictly prohibited."
- Policy: Prohibition included in revised Conflict of Interest Policy.

DoD Policy: Cornell Status

Malign Foreign Talent Recruitment Programs:

- Same as CHIPs

Screening:

- Cornell has a subscription to Visual Compliance – a software program that screens all U.S. restricted party lists. Currently, screening is done on:
  - All collaborators (OSP, OVPIA, Procurement)
  - All new hires
  - COI disclosures – reported foreign entities

Response to Pre-Award Mitigation Letters

- Cornell has received two Pre-Award Mitigation Letters

Updates and Ongoing Efforts

Discussion

Updates

- **The National Science Foundation issued updated requirements** for research security assessments, training, and documentation.
  - As of Oct. 10, 2025, Research Security training must have been completed by all senior/key personnel on NSF proposals in the 12 months prior to proposal submission. Cornell is transitioning to using NSF's SECURE consolidated Research Security Training. It has been accepted by NSF, DOD, DOE and NIH. All researchers will be assigned the training September 2, 2025.
- **The National Science Foundation issued updated requirements** for documentation collection and review.
  - As of Oct. 10, 2025, NSF proposers and recipients are required to maintain supporting documentation, including copies of contracts, grants, or any other agreements specific to foreign appointments, employment with a foreign institution, participation in a foreign talent recruitment program and other information reported as current and pending (other) support for all senior/key personnel that must be available to NSF upon request. Proposers and recipients are expected to review requested supporting documentation for compliance with NSF award terms and conditions. We are working with our software developers to implement features into COI System for uploading contracts to comply with this requirement.

Updates

- **The National Institutes of Health issued updated requirements** for training on other support.
  - As of October 1, 2025, recipients must implement trainings, in addition to maintaining a written and enforced policy, on requirements for the disclosure of other support to ensure Senior/Key Personnel fully understand their responsibility to disclose all resources made available to the researcher in support of and/or related to all of their research endeavors, regardless of whether or not they have monetary value and regardless of whether they are based at the institution the researcher identifies for the current grant. The SECURE Training will satisfy this requirement.

- **The United States Department of Agriculture issued updated requirements** for research security which require a number of certifications and disclosures related to collaborations with foreign entities and persons. America First Memorandum for USDA Arrangements and Research Security

Research Security Efforts

Research Security Compliance Committee

- Training Working Group
- Implementation of new rules and guidance on research security
- Identifies and updates gaps related to research security

Outreach

- How to communicate all the new requirements and issues to faculty and staff?
  - Newsletters
  - OSP Roundtables
  - Message from leadership
  - Department-specific outreach

Thank You