

# Texas A&M Research Security and Export Controls Office (RESEC)

*April 17, 2025*



# Are you here for RCR credit?

*To request credit for 1 hour of Face-to-Face Responsible Conduct of Research Training from today's presentation, please email our office at [RCR@tamu.edu](mailto:RCR@tamu.edu). (Please note, this requirement is typically only required of graduate students and postdocs, per TAMU SAP 15.99.99.M0.04.)*

## Upcoming Responsible Conduct of Research Sessions:

- Wednesday, June 4, 2025– 1 hour offered - Virtual
  - 11:00-12:00pm– RCR – Collaborative Research: Conflict of Interest/Conflict of Commitment
- Tuesday, June 24, 2025– 1 hour offered - Virtual
  - 10:00-11:00am– RCR – Human Subjects
- Thursday, June 26, 2025– 1 hour offered - Virtual
  - 10:00-11:00am– AnSRS4U: Export Controls & Prohibited Technologies
- Thursday, July 1, 2025– 1 hour offered - Virtual
  - 10:00-11:00am– RCR – Export Controls
- Wednesday, July 16, 2025– 1 hour offered - Virtual
  - 10:00-11:00am– RCR – Biosafety
- Thursday, August 21, 2025– 4 hours offered – In-Person
  - 10:00-2:30pm– RCR – 4 hour In-Person Workshop (must attend all 4 hours)



# International Activities and Collaborations

Universities such as Texas A&M are actively responding to concerns from federal agencies and sponsors regarding foreign influence in academic research.

This influence may range from conflicting commitments of researchers to foreign entities to the misappropriation of research results and intellectual property.

While we value and encourage international collaborations that promote openness in research and scholarship, Texas A&M must comply with U.S. laws and agency regulations that govern how we manage and report international engagements. Understanding the regulatory environment, the risks, and importance of transparency is an individual responsibility as well as an organizational commitment.

Texas A&M encourages its faculty to establish global engagements in the pursuit of mutually beneficial fundamental scientific inquiries, cultural, or educational opportunities.



# How did we get here?



- Inappropriate sharing of grant applications and other disruptions to the peer review process



- Conducting the same, or similar, research at two institutions (shadow lab) and/or having the same project supported by both U.S. federal funds and foreign funds



- Incomplete disclosure of relationships with foreign governments or institutions to R&D sponsors and the investigator's home institution

# Dr. Charles Lieber

- Dr. Charles Lieber
  - Harvard Professor
  - 15M+ in NIH and DoD research funding
  - 2011: named the leading scientist in the world for the decade 2000-2010 based on the impact of his scientific publications
  - Published 400+ papers in peer-reviewed journals; principal inventor on 50+ US patents & applications; too many awards to list
- Wuhan University of Technology (China)
  - Strategic scientist beginning in 2011
  - Thousand Talents Contract
    - Wuhan paid Dr. Lieber \$50K/month; \$150K+ living expenses; \$1.5M research
    - Dr. Lieber agreed to work for Wuhan “not less than 9 months a year”
    - He traveled from Wuhan to Boston with bags of cash containing between \$50,000 and \$100,000 (which was never disclosed to the IRS)
- Federal Investigators and Harvard
  - Investigations began in 2018
    - Included DoD asking about talent awards and NIH asking Harvard about Dr. Lieber’s foreign affiliations
  - He lied to the Feds and to Harvard about having a talent award and his work for Wuhan
    - He claimed he was never asked to participate in the Thousand Talents Program, and wasn’t sure how China categorized him
    - But an email was found from Wuhan to Lieber dated 2012 that included a Thousand Talents contract
  - He denied any knowledge of his bank accounts in China or the money from Wuhan
- January 2020: Dr. Lieber was arrested and charged with 2 federal counts of making materially false, fictitious and fraudulent statements
- December 2021: Convicted of 6 felonies in Federal Court, including lying to federal authorities and failing to report the additional income he received from Wuhan
- September 2022: U.S. Federal Court denied his request to overturn his conviction or his request for a new trial
- January 2023: sentencing hearing is scheduled
- April 26, 2023: sentenced to 6 months of house arrest





# Pumpkins Too?

Congrats Charlie Lieber for the win in 2020 and largest pumpkin ever weighed at Frerichs.



Largest pumpkin in Massachusetts in 2014 weighing in at 1,870 lbs



# Brief History and Timeline

- **August 2018: NIH Director Dr. Frances Collins letter**
  - Laid the groundwork for discussions on research security
  - Dr. Collins sent a letter to over 100 research institutions regarding researchers participating in internationally based research and/or academic outside activities that had not been disclosed
  - Concerns that this undisclosed support was the source of intellectual property diversion away from the US
  - Term “foreign influence” was used to define this concern
- **December 2019: JASON Report**
  - JASON advisory group is an elite group of scientists that advise the US Government on matters of science and technology
  - Report further clarified the risks created where there is a lack of disclosure, specifically in the context of Intellectual Property theft and Research Security
  - Include “Conflict of Commitment” under the Research Security Umbrella
- **January 2021: National Security Presidential Memo – 33 (NSPM-33)**
  - Mandated the establishment of research security programs to protect against foreign government interference and exploitation at research institutions receiving federal funds in excess of \$50M per year
- **January 2022: Guidance for Implementing NSPM-33**
- **August 2022: CHIPS and Science Act of 2022**
  - Includes Research Security Requirements
- **March 2024: JASON Report**
  - At NSF’s request to comment on specific steps NSF might take to identify sensitive areas of research and describe processes to address security in those areas
- **July 2024: Office of Science & Technology**
  - Posted guidelines that confirmed the 4 mandatory program elements required for a compliant research security program

# National Security Presidential Memorandum 33 (NSPM-33)

## Guidance for Implementing NSPM-33 on National Security Strategy for United States Government-Supported Research and Development – January 2022

- Strengthen protections of U.S. Government-supported R&D against foreign government interference and misappropriation, while maintaining an open environment to foster research discoveries and innovation that benefit the United States and the world.
- Outlined commitments in the following areas:
  - Engaging regularly with the research community and other stakeholders to share information
  - Standardizing disclosure information to assess potential conflicts of interest and conflicts of commitment
  - Coordinating agency policy development for researcher digital persistent identifiers
  - Developing research security program standards
- Specifically regarding research security programs, NSPM-33 directs research institutions receiving more than \$50M in Federal science and engineering support in the prior 2 fiscal years to establish a research security program that includes 4 elements:
  - Cybersecurity
  - Foreign Travel Security/Training
  - Research Security Training
  - Export Control Training



# NSPM-33

## Cybersecurity

### Previous Draft Guidance:

- Must implement baseline safeguarding protocols and procedures for information systems used to store, transmit, and conduct federally funded R&D. The following protocols are required pursuant to the draft guidance:
  - Limit information system access to authorized users and processes acting on behalf of authorized users, or devices (including other information systems), as described in Office of Management and Budget Memorandum [M-21-31](#) on Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.
  - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
  - Verify and control/limit connections to, and use of, external information systems.
  - Control any non-public information posted or processed on publicly accessible information systems.
  - Identify information system users and processes acting on behalf of users, or devices.
  - Authenticate (or verify) the identities of those users, processes, and devices, as a prerequisite to allowing access to organizational information systems.
  - Monitor, control, and protect organizational communications (information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
  - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
  - Identify, report, and correct information and information system flaws in a timely manner.
  - Provide protection from malicious code at appropriate locations within organizational information systems.
  - Update malicious code protection mechanisms when new releases are available.
  - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, and executed.
- Must follow applicable cybersecurity requirements and controls beyond these baseline requirements for research involving classified information, controlled unclassified information (CUI), commercially sensitive information, or information that, if inadvertently or intentionally released, may harm US Government rights.

### UPDATED Final Guidance:

- Final guidelines require implementation of a cybersecurity program 1 year after publication of the final National Institute of Standards and Technology (NIST) cybersecurity resource. *This resource has not yet been published.*

# NSPM-33

## Foreign Travel Security

### **Previous Draft Guidance:**

- Establish and maintain international travel policies for covered individuals engaged in federally funded R&D who are traveling internationally for organization business, teaching, conference attendance, research purposes, or who receive offers of sponsored travel for research or professional purposes.
- International travel policies and procedures must include:
  - Maintenance of an organizational record of covered international travel by covered individuals engaged in federally funded R&D
  - A disclosure and authorization requirement in advance of international travel
  - Mandatory applicable security briefings, and advice regarding electronic device security (e.g. smartphones, laptops) prior to covered international travel, or to travel including electronic devices utilized for federally funded R&D or bought with Federal funding

### **UPDATED Final Guidance:**

- Implement federal foreign travel security training to covered individuals within 1 year of availability and at least every 6 years
- Organizational record of covered individuals international travel when an agency determines security risks warrant travel reporting for an R&D award.

*Note: The federal government resource that institutions may use in providing mandated foreign travel security training is not yet developed.*



# NSPM-33

## Research Security Training

### Previous Draft Guidance:

- Must implement research security training as a component of research security programs; elements include understanding the importance of research security; disclosures; proper use of funds; international collaborations; intellectual property and data requirements; cybersecurity, international travel practices
- In the event of a research security breach finding, must conduct tailored training related to the finding as a component of the organization's response, and keep a record of such trainings for affected individuals.

### UPDATED Final Guidance:

- Must implement research security training as a component of research security programs in one of the following ways:
  - Certification that covered individuals have completed the training modules that NSF published:
    - NSF Module 1 – Introduction to Research Security
    - NSF Module 2 – The Importance of Disclosure
    - NSF Module 3 – Manage & Mitigate Risk
    - NSF Module 4 – The Value of International Collaboration
  - Certification that covered individuals have completed a research security program that:
    - Includes explicit examples of behaviors that have resulted in “known improper or illegal transfer of U.S. government-supported R&D in the context of the research environment, as described in the covered institution by federal research agencies” and
    - Communicates to Covered Individuals “the importance of U.S. research participation in global discoveries, including attracting foreign talent to U.S. research institutions, as a core principle of maintaining international leadership and national security”
    - \*NEW\* TrainTraq Course 2114875: Research Security Training (Combined)

# NSPM-33

## Export Control Training

### Previous Draft Guidance:

- Must provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators, and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists. The training must emphasize that the “fundamental research” exception has explicit limitations. For example, federally funded R&D of “applied” energy technologies (i.e., “applied research”), many with dual-uses (civilian and military), fall outside of any exception and are subject to such laws.

**UPDATED Final Guidance:** Final guidelines require that covered individuals who perform R&D involving export-controlled technologies have completed training on U.S. export control and compliance requirements. This requirement can be met by one of the following:

- requiring covered individuals to complete relevant trainings administered by the Bureau of Industry and Security of the Department of Commerce and that each relevant covered individual has completed such training. Additionally, the Directorate of Defense Trade Controls at the Department of State has publicly available resources to assist an institution in developing its own in t compliance programs; **or**
- requiring covered individuals to complete training on complying with:
  - (1) U.S. export control and compliance requirements; and
  - (2) requirements and processes for reviewing foreign sponsors, collaborators, and partnerships.





# CHIPS and Science Act of 2022

## Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022

- designed to boost U.S. competitiveness, innovation, and national security

### **Includes several provisions specific to national research security:**

- Prohibition of malign foreign government talent recruitment programs
- Requirements to establish a research security and integrity information sharing and analysis organization
- Mandates research security training requirements for all covered personnel
- Inclusion of research security training as part of RCR training
- Reporting on foreign financial transactions and gifts
  - Must report annually on foreign financial transactions on amounts over \$50,000 from countries of concern
- Prohibition of Confucius Institutes

# Department of Energy

## Research Security Training

### **Starting for Proposals Submitted on or after May 1, 2025:**

- As a reminder, research security training is mandated for individuals involved in federally funded research by U.S. federal regulations such as the [CHIPS and Science Act](#) and [National Security Presidential Memorandum 33](#) (NSPM-33).
  - Within 12 months PRIOR to an application submission, covered individuals must complete research security training
  - Covered individuals must certify that they have completed the training via the Current and Pending Support disclosure certification
  - Institutions must certify that all covered individuals who are listed on the application have completed the research security training
- Covered Individuals: any principal investigator (PI); project director (PD); co-principal investigator (Co-PI); co-project director (Co-PD); project manager; and any individual regardless of title that is functionally performing as a PI, PD, Co-PI, Co-PD, or project manager, as well as anyone designated by DOE.

# Department of Energy

## Research Security Training

### Options for meeting the Research Security Training requirement:

1. Complete all 4 of the following modules:
  - TrainTraq course 2114744 NSF Module 1 – Introduction to Research Security
  - TrainTraq course 2114745 NSF Module 2 – The Importance of Disclosure
  - TrainTraq course 2114746 NSF Module 3 – Manage & Mitigate Risk
  - TrainTraq course 2114747 NSF Module 4 – The Value of International Collaboration

**OR**

2. Complete TrainTraq Course 2114875: Research Security Training (Combined)

### Frequency

Possibly annual due to the CHIPS requirement language of “within 12 months of submitting a research and development application to a federal agency.”

# System Regulation 15.01.03, Financial Conflicts of Interest in Sponsored Research

**Significant financial interest (SFI)** – a financial interest, including but not limited to one or more of the following interests of the investigator (and those of the investigator's covered family members), that reasonably appears to be related to the investigator's institutional responsibilities:

- (a) With regard to any publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the 12 months preceding the disclosure and the value of any equity interest in the entity as of the date of disclosure, when aggregated, exceeds \$5,000.
- (b) With regard to any non-publicly traded entity, a significant financial interest exists if the value of any remuneration received from the entity in the 12 months preceding the disclosure, when aggregated, exceeds \$5,000.
- (c) Intellectual property and royalty interests (e.g., patents, copyrights), upon receipt of income related to such rights and interests.
- (d) The occurrence of any reimbursed or sponsored travel (i.e., that which is paid on behalf of the investigator and not reimbursed to the investigator so that the exact monetary value may not be readily available), related to their institutional responsibilities; provided, however, that this does not include travel that is reimbursed or sponsored by a federal, state or local government agency, an institution of higher education as defined at 20 U.S.C. §1001(a), an academic teaching hospital, a medical center or a research institute that is affiliated with an institution of higher education.
- (e) Gifts, when the value of a single gift received by the investigator or a covered family member in the preceding 12 months exceeds \$250, or when the aggregated value of multiple gifts received from a single entity within the preceding 12 months exceeds \$250, excluding gifts received from a covered family member.
- (f) Any fiduciary position held by an investigator or a covered family member in a for-profit or nonprofit entity in the preceding 12 months, including a position as a member of the board of directors, an officer or other executive or management position for which the investigator or covered family member received any form of remuneration or reimbursement for expenses.



# System Regulation 31.05.01, Faculty Consulting and/or External Professional Employment

- Updated April 2020
  - Faculty consulting and/or external professional employment – any work, advice or service related to a faculty’s field of discipline for which a system faculty member receives compensation, services, goods, or any other item of value. The term includes, but is not limited to, any fee-for-service or equivalent relationship with a third party, employment by an individual, self employment, or employment by an entity in which the faculty member is a principal owner. **In addition, the provision of certain types of scholarly or research expertise to foreign entities without compensation constitutes “faculty consulting and/or external professional employment” for purposes of this regulation. These types include, but are not limited to, participation in scholarly or scientific research projects or publications required to be disclosed to any agency of the U.S. government, as well as communication of any information subject to export control, publication restriction or confidentiality agreement.**
- Minor tweaks to underlined text in July 2023 as follows:
  - **While not technically “faculty consulting and/or external professional employment,”** the provision of certain types of scholarly or research expertise to foreign entities without compensation **must be disclosed to the member institution for purposes of System Policy 15.02, Export Control Program Management and System Regulation 15.05.04, High Risk Global Engagements and High Risk International Collaborations.** These types include, but are not limited to, participation in scholarly or scientific research projects or publications required to be disclosed to any agency of the U.S. government, as well as communication of any information subject to export control, publication restriction or confidentiality agreement.
- \* *Virtually identical definition for External Employment under System Regulation 31.05.02 External Employment*

# System Regulation 15.05.04 High Risk Global Engagements and High Risk International Collaborations

- New regulation effective August 18, 2022; University rule April 6, 2023
- What is a High Risk Global Engagement?
  - Contracts with one or more Foreign Persons based outside the United States in a Country of Concern
  - Includes contracts that require participation with Foreign Persons based in a Country of Concern
- What is a High Risk International Collaboration?
  - Old Definition: any of the following relationships with Foreign Persons based outside the United States in a Country of Concern: student and faculty exchanges; placements abroad; unfunded research relationships; technical assistance; unfunded professional development, training, and services; unfunded outside appointments, honorary positions, peer review, or distinguished positions; unfunded outside support including but not limited to lab space or other resources, provided either physically or virtually; activities with Foreign Persons traditionally compensated by a payment, honorarium, or paid travel expenses.
  - New Definition: relationships and activities with Foreign Persons based outside the United States in a Country of Concern as described in Section 238(b)(1) of the Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025 (Public Law 118-159). This includes gifts from entities associated with a Country of Concern.
- Currently, what are the Countries of Concern?
  - China (includes Hong Kong), Russia, Iran, and North Korea
  - Venezuelan politician Nicolás Maduro (Maduro Regime) and Cuba recently added; Macau recently removed
- What does this mean?
  - High risk global engagements and high risk international collaborations require additional reviews and approvals, including final approval from the Texas A&M System Vice Chancellor for Research.

# System Regulation 15.05.04

## High Risk Global Engagements & High Risk International Collaborations

- System Regulation updated February 28, 2025:
  - Time Deadline
    - RESEC must submit to System at least 10 business days in advance of the activity; our draft rule will require an additional 10 days, for a total of 20 days
  - Disciplinary actions
    - We must include a process for disciplinary actions for non-compliance
  - System employees are prohibited from accepting gifts or traveling to a Country of Concern for professional purposes
  - System employees are prohibited from entering into HRGE and participating in HRIC with entities on the most recent list developed by Section 1286 of the NDAA (Public Law 115-232)

# System Regulation 15.05.04

## Countries of Concern

### Current Countries of Concern:

- China (includes Hong Kong)
- Cuba
- Iran
- North Korea
- Russia
- Venezuelan politician Nicolás Maduro (Maduro Regime)



# Texas Governor's Executive Order

## GA-48

- Issued November 19, 2024
- Hardening of state government to protect national security
- Key Elements:
  1. Certification that vendors are not listed on various prohibited vendor lists
  2. No personnel can accept gifts or travel to (for professional purposes) a country on the foreign adversaries list
  3. Applicants must attest they are not connected to a country on the foreign adversaries list
  4. Employees must provide notification of personal travel to a foreign adversary nation prior to travel and a post-travel brief outlining details of the trip
  5. Ensuring personnel that have access to critical infrastructure can maintain security and do not have criminal history or connections to foreign adversaries
  6. The reporting of foreign gift and contract disclosures to the THECB
  7. Prohibition of faculty and employees taking part in recruitment programs from foreign adversary nations
- Implementation team has been established and are working through all 7 elements.

# What does this mean?

**Any global engagement or international collaboration with a country of concern will require an additional approval from the System Vice Chancellor for Research**

- **Travel**
  - *Remember, GA-48 currently prohibits travel to a COC for professional purposes*
- **Sponsored projects**
- **External Employment/Outside Activities**
- **Appointments (including honorary positions)**
- **Collaborations (funded or unfunded)**
- **Agreements/Awards (funded or unfunded)**

# Risk Matrices

## DoD

- Policy on Risk-based security reviews of fundamental research
- Decision matrix to inform fundamental research proposal mitigation
  - Participation in FTRPs; current/prior funding sources from COC; patents filed in a COC; associations/affiliations with Entity List
- As of April, 2024 COGR Survey: 80% of mitigation plans were Army ARL, followed by DARPA, Air Force, and ONR.

## DOE

- Public version of the DOE risk criteria is in process
- Review associations/affiliations/possible FTRP involvement up to 10 years back
- May review awardee personnel's higher education in a foreign country

## NIH:

- Decision matrix as a guide to assist NIH in reviewing grant applications and ongoing awards
  - Participation in FTRPs; foreign funding; and affiliations with foreign institutions/entities
- Reviews back 5 years

## NSF:

- Least restrictive as of now
- Reviews back to NSPM-33 release (2022)

# DoD Matrix

**Table 1: Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions**  
**Factors for Assessing a Covered Individual’s Associations, Affiliations, Collaborations, Funding, and the Policies of the Proposing Institution that Employs the Covered Individual**

	Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
<b>Prohibited factors</b>	<p><b>For the Period after 9 Aug 2024</b></p> <p>Indicators of participation in a malign foreign talent recruitment program (MFTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p>Policy of Proposing Institution employing the covered individual does not prohibit participation in a MFTRP.</p>			
<b>Factors discouraged by DoD policy, mitigation measures required, rejection of proposal required if no mitigation possible</b>	<p><b>For the period after 9 Aug 2022<sup>1</sup>:</b></p> <p>Indicator(s)<sup>2</sup> of participation<sup>3</sup> in a foreign talent recruitment program (FTRP) meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	Indicator(s) that the covered individual is currently receiving funding from a Foreign Country of Concern (FCOC) or a FCOC-connected entity.	Patent application(s) or patent(s) not disclosed in proposal, that resulted from research funded by the U.S. Government (USG), that were filed in an FCOC prior to filing in the U.S. or filed on behalf of an FCOC-connected entity.	<p><b>For the period after 9 Aug 2022:</b></p> <p>Indicator(s) of association with an entity on: the U.S. Bureau of Industry and Security (BIS) Entity List,<sup>4</sup> the Annex of Executive Order (EO) 14032<sup>5</sup> or superseding EOs, Sec. 1260H of the National Defense Authorization Act (NDAA) for FY 2021,<sup>6</sup> or Sec. 1286 of the NDAA for FY 2019, as amended.<sup>7</sup></p> <p><b>For the period after 10 Oct 2019:<sup>8</sup>:</b></p> <p>Indicator(s) of affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p>
<b>Mitigation measures recommended</b>	<p><b>For the period between 10 Oct 2019<sup>9</sup> and 9 Aug 2022:</b></p> <p>Indicator(s) of participation in an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p><b>For the period after 9 Aug 2022:</b></p>	<p><b>For the period between 10 Oct 2019 and 9 Aug 2022:</b></p> <p>Indicator(s) that the covered individual received funding from a FCOC or an FCOC-connected entity.</p>	<p>Patent application(s) or patent(s) disclosed in proposal, resulting from research funded by the USG, that were filed in an FCOC prior to filing in the U.S. or on behalf of an FCOC-connected entity.</p>	<p><b>For the period between 10 Oct 2019 and 9 Aug 2022:</b></p> <p>Indicator(s) of association with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p> <p><b>For the period prior to 10 Oct 2019:</b></p>

	Policy of proposing institution employing each covered individual does not prohibit participation in a MFTRP.			Indicator(s) of an affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.
<b>Mitigation measures suggested</b>	<p><b>For the period after 10 Oct 2019:</b></p> <p>Covered individual’s co-author(s)<sup>9</sup> on publications in scientific and engineering (S&amp;E) journals are participants in an MFTRP or an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p> <p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) of participation in a FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	<p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) that the covered individual received limited or partial funding from a FCOC or an FCOC-connected entity.</p>	<p>Patent application(s) or patent(s) not disclosed in fundamental research project proposal, that resulted from research funded by the USG, that were filed in a non-FCOC prior to filing in the U.S. or on behalf of an entity in a non-FCOC.</p> <p>Co-patent applicant with a person on the U.S. BIS Denied Persons List.<sup>10</sup></p>	<p><b>For the period after 10 Oct 2019:</b></p> <p>Covered individual’s co-author(s) on publications in S&amp;E journals are affiliated with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p> <p>Covered individual is a co-author on a publication in an S&amp;E journal with a person on the U.S. BIS Denied Persons List.</p> <p><b>For the period prior to 10 Oct 2019:</b></p> <p>Indicator(s) of association with an entity on: the U.S. BIS Entity List, the Annex of EO 14032 or superseding EOs, Sec. 1260H of the NDAA for FY 2021, or Sec. 1286 of the NDAA for FY 2019, as amended.</p>
<b>No mitigation needed</b>	<p>No indicator(s) of participation in an MFTRP; or</p> <p>No indicator(s) of participation in an FTRP meeting any of the criteria in Sec. 10638(4)(A)(i)-(ix) of the CHIPS and Science Act of 2022.</p>	No indicator(s) that the covered individual is receiving or has received funding from an FCOC or an FCOC-connected entity.	All patent application(s) or patent(s), resulting from research funded by the USG, have been filed in the U.S. prior to filing in any other country.	No indicator(s) of any association or affiliation with an entity on: the U.S. BIS Entity List, the Annex of EO 14032, or superseding EOs, Sec. 1260H of the NDAA for FY 2021, Sec. 1286 of the NDAA for FY 2019, as amended, and no indicator(s) of publication in S&E journals co-authored with an individual on the U.S. BIS Denied Persons List.

# Risk Matrices

## Summary Comparison Chart

Agency	Risk Factor 1	Risk Factor 2	Risk Factor 3	Risk Factor 4	Co-authorship a factor?	How far back are they looking?
DoD (Including DARPA)	Foreign Talent Recruitment Program participation	Funding from Foreign Country of Concern	Patent applications of patents filed outside the U.S., particularly in a Foreign Country of Concern	Association or affiliation with entities on Entity List	Yes	Some factors from October 10, 2019 (Griffin letter); others from August 9, 2022 (CHIPS Act)
US Army	Foreign Talent Recruitment Program participation	Affiliated with Denied Entities	Funding from strategic competitors	Affiliation, association, or collaboration with strategic competitors	Yes	Not specified
DOE	Foreign Talent Recruitment Program participation - foreign funding sources and certain convening behaviors associated with patenting	Foreign ownership or control, criminal or regulatory issues, the supply change for any sensitive equipment/supplies, and ties to entities on specified lists	Risk Factors tied to Date of Activity or Relationship	Technology Considerations - emerging or critical technologies	Possibly (not stated in policy but verbally stated on several occasions that they "may" look at co-authors)	Unclear, but likely 2019; they have verbally mentioned potentially 10 years back
NIH	Foreign Talent Recruitment Program participation	Undisclosed foreign funding, particularly from a Foreign Country of Concern	Undisclosed affiliations with foreign institutions or entities, particularly with a Foreign Country of Concern	N/A	No, if not directly related to NIH-funded work	5 years
NSF (Quantum proposals only)	Active appointments with positions with or research support from U.S. proscribed parties and any party to a MFTRP	Non-disclosures of appointments, activities, and sources of research support	Potential foreseeable national security applications of the research	N/A	No	Undisclosed information will be examined from January 2022 (NSPM-33 Implementation Guidance)

# What can you do to remain compliant?

- Watch for updates!
  - We have several workgroups reviewing new and upcoming requirements
- Disclose, and obtain required University approvals
- Traveling or Collaborating Internationally?
  - Ensure you have the proper approvals, including export control and IT
- Financial Conflict of Interest
  - Regulation relatively unchanged since 2012
  - Review not only for financial conflicts, but also export controls and research security concerns
- Conflict of Commitment and Faculty Consulting and/or External Employment
  - Faculty: required approval for any work, advice or service related to a faculty's field of discipline for which compensation is received
  - Staff (includes faculty when external employment is not directly related to their professional discipline): required approval for any work, advice or service for which a system employee receives compensation, services, goods, or any other item of value.
- Global Engagements and International Collaborations
  - Ensure you receive University approvals, and allow additional time for System review and approval



**Questions?**