



Office of Research Protections, Research Security & Trade Compliance

Research Security Overview

Allen A. DiPalma, MBA
Executive Director

December 5, 2025



©2007 Michael G. W.



Webinar Agenda

- Background
- Industry Case Studies
- NSPM-33 and the CHIPS Act Provisions
- Malign Foreign Talent Recruitment Programs
- Research Security Training Requirements
- Risk Mitigation Requests
- Cybersecurity
- Additional Research Security Topics on our Radar

Research Security Background

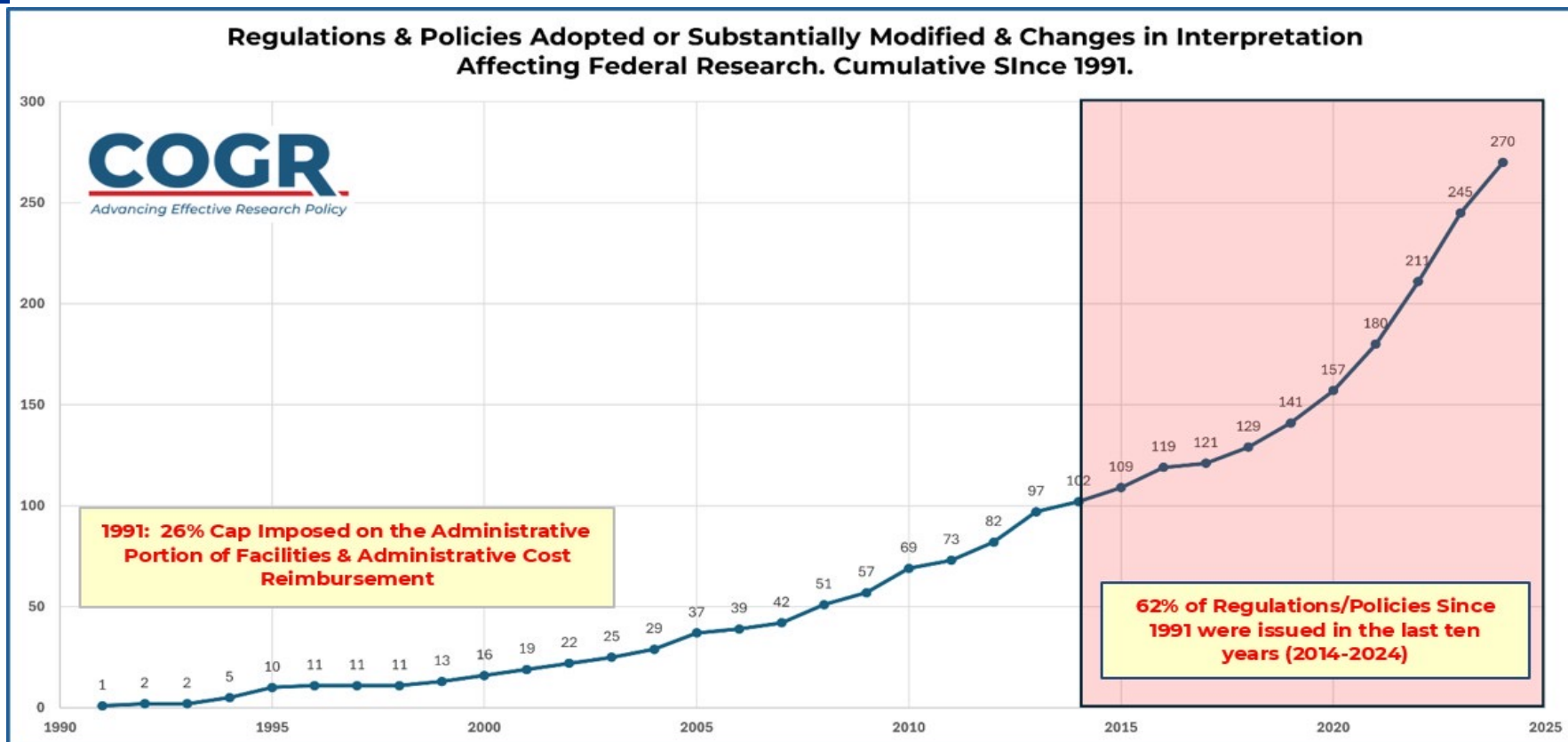
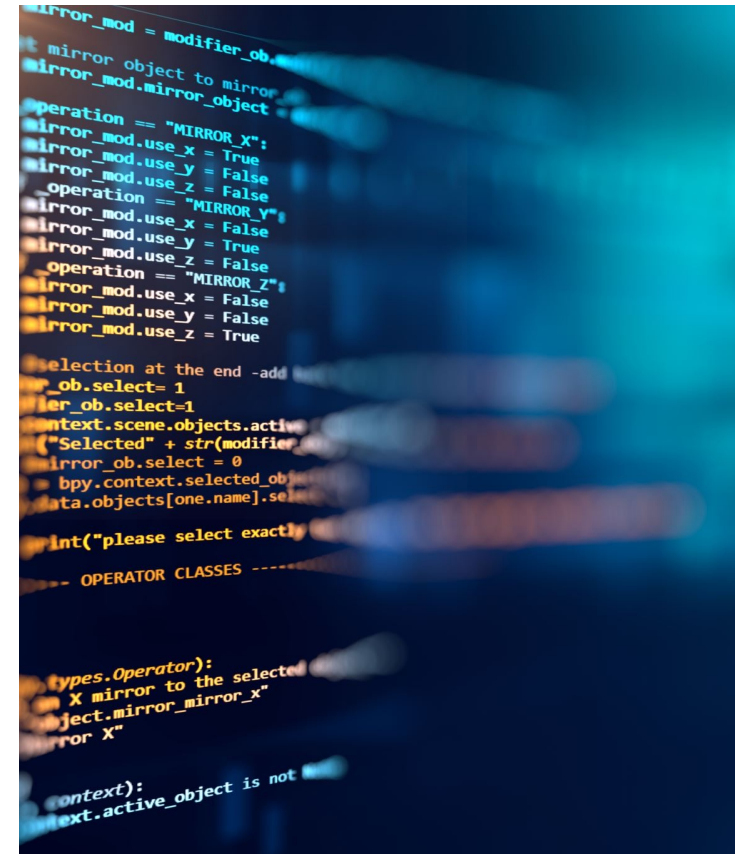


Figure 1. Regulations & Policies Adopted or Substantially Modified & Changes in Interpretation Affecting Federal Research. Cumulative Since 1991.

Research Security Defined

- Research Security is the protection of the research enterprise against threats such as misappropriation, violations of research integrity, and foreign government interference.
- It involves safeguarding intellectual property, sensitive data, and technological advances from unauthorized access or theft.
- Research security policies are often developed in collaboration with government agencies, law enforcement, and intelligence communities to ensure the national defense and economic security are not compromised by the research activities.

Source: Microsoft Co-Pilot, March 17, 2024



Background 2017-2021

- FBI Director advises Congress that Chinese students pose a counterintelligence threat.
- The term “non-traditional collector” is coined to describe this new threat.
- Federal agencies begin to scrutinize faculty other support and bio sketches for unreported foreign engagements.
- Universities begin to analyze COI/COC data to confirm foreign engagements.
- Universities and federal agencies take action against those who do not disclose foreign engagements.

COGR
Council On Governmental Relations

In the News – Why This Matters

THE WALL STREET JOURNAL

U.S. Reaches Settlement on Undisclosed Chinese Funding of Scientists

[The Van Andel Research Institute, Michigan](#)

The Washington Post

Accused of fraud, Kansas researcher denies working for a Chinese university as he fights federal charge

[Kansas State University](#)

TIME

Emory University Fires 2 Neuroscientists Accused of Hiding Chinese Ties

TheScientist
EXPLORING LIFE, INSPIRING INNOVATION

UCSD Eye Doctor Resigns After Investigation into Ties with China

[University of California at San Diego](#)

Medscape

Major Cancer Center's CEO, Staff Resign over Chinese Payments

[Moffitt Cancer Center, Florida](#)

Science
AAAS

Exclusive: Major U.S. cancer center ousts 'Asian' researchers after NIH flags their foreign ties

[MD Anderson Cancer Center, Texas](#)

Bloomberg

U.S. Charges Chinese Professor Accused of Theft to Help Huawei

[University of Texas at Arlington](#)

All logos on this page are referenced for educational, non-commercial, and editorial purposes only.

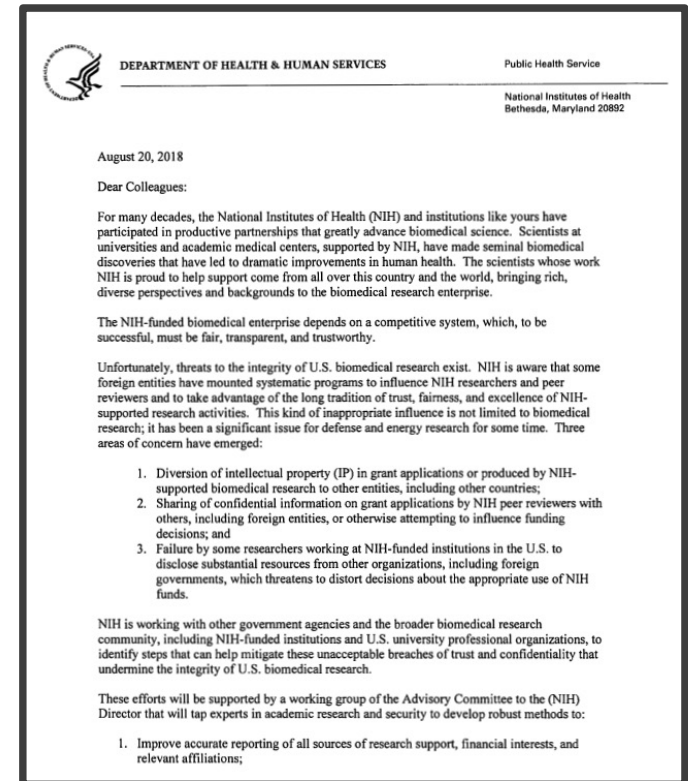
Federal Agency Actions

- **Problems:**

- IP Theft and Diversion ★
- Policy Influence
- Peer Review Confidentiality
- Disclosure of Foreign Engagements ★

- **Response:**

- Dear Colleague Letters (NIH, NSF, DOD)
- Special Reports (NIH, NSF JASON Report)
- Reminders to grantees RE: other support, COI, COC, foreign components
- Limits on participation in Foreign Talent Recruitment Programs (NSF, DOE)



Foreign Talent Recruitment Programs

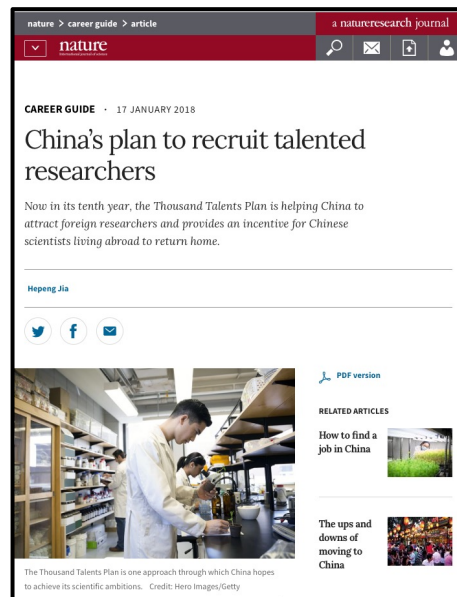
- An effort directly or indirectly organized, managed, or funded by a foreign government or institution to recruit S&T professionals or students (regardless of citizenship or national origin, and whether having a full-time or part-time position).

Source: NSPM-33



Foreign Talent Recruitment Program Pivot

JANUARY 2018



OCTOBER 2018



FEBRUARY 2019



Research Integrity Principles

OSTP Describes Research Integrity as:

- Openness and Transparency
- Accountability and Honesty
- Impartiality and Objectivity
- Respect
- Freedom of Inquiry
- Reciprocity
- Merit-Based Competition



FTRP Research Integrity Violations

1. Effort commitments that conflict with U.S. university primary appointments
2. One-sided contract terms that do not recognize previous U.S. taxpayer support or IP rights
3. Requirements to own all research results, which interferes with the ability to freely publish
4. Nondisclosure clauses that keep existence of contracts from universities and federal agencies
5. Undisclosed use of U.S. university names, facilities, and IP
6. Difficult termination clauses that favor the talent program
7. Publication authorship requirements that conflict with accepted industry standards
8. Requirements to recruit students and researchers and, in some cases, relocate laboratories from U.S. locations to other countries

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs
Rob Portman, Chairman
Tom Carper, Ranking Member

Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans

STAFF REPORT

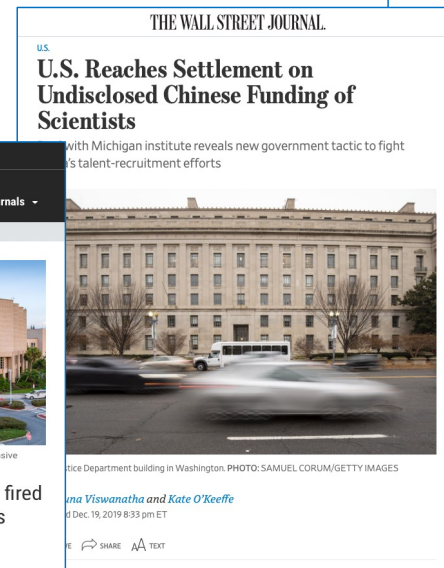
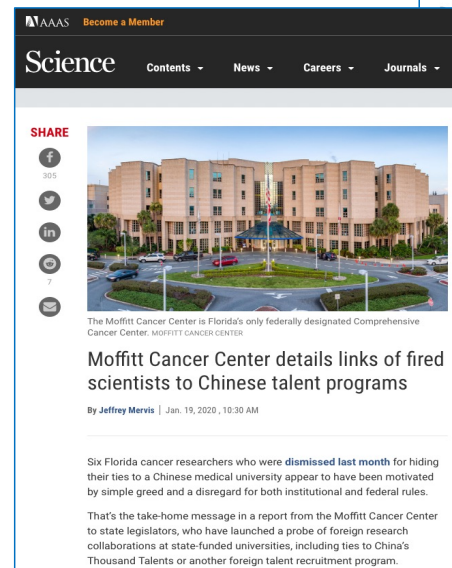
PERMANENT SUBCOMMITTEE ON
INVESTIGATIONS

UNITED STATES SENATE



Managing the Risks: Public Examples

- Reputational
- Financial
- Legal
- Individual
- National Security



Industry Case Studies

Dr. Charles Lieber Case: Background

- Dr. Lieber was PI of the Lieber Research Group at Harvard which specialized in nanoscience.
- He was also the Chair of the Chemistry Department and held a full-time appointment.
- Dr. Lieber received > \$15M in grant funding from NIH and DOD.
- Participated as Strategic Scientist for Wuhan University of Technology (WUT) under a Thousand Talent Program (TTP) award from 2012 through 2017.
- He was paid \$50K per month in salary support, \$158K in annual living expenses, and given 1.5M to start a lab at WUT.
- Dr. Lieber was obligated to work for WUT no less than 9 months of the year.
- Dr. Lieber told federal authorities in 2018/2019 that he had no involvement with the TTP or WUT.
- Harvard certified to NIH that he had no formal association with TTP or WUT.

Source: DOJ Website: <https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related>

Dr. Charles Lieber Case: Conclusion

➤ Main Issues:

- Foreign Talent Program Participation (TTP)
- Foreign Appointment (Strategic Scientist for WUT)
- Financial Conflict of Interest Disclosure (\$50K per month)
- Conflict of Commitment Disclosure (9-month appointment at WUT)
- Other Support Disclosures (NIH, DOD)

➤ Consequences:

- Individual: Dr. Lieber was convicted on 6 counts (False Statements, income tax, foreign bank accounts)
- Reputational: Dr. Lieber (directly), Harvard (by association)
- Legal: Non-disclosure led to Harvard violation of grant COI terms
- National Security: Transfer of STEM expertise to foreign lab/program

Dr. Gang Chen: Background

- Dr. Gang Chen is a professor and researcher at MIT where he serves as Director of the MIT Pappalardo Micro/Nano Engineering Laboratory and Director of the Solid State Solar Thermal Energy Conversion Center.
- Since 2013, Dr. Chen received > \$19 million in grants from various federal agencies.
- Since 2012, Dr. Chen allegedly held various appointments with the PRC designed to promote the PRC's S&T development.
- He was alleged to have participated in at least two PRC Talent Recruitment Programs.
- Since 2013, Dr. Chen received approximately \$29 million of foreign funding including \$19 million from PRC's Southern University of Science and Technology.
- From 2017 to 2019, Dr. Chen obtained research funding from the U.S. Department of Energy and allegedly failed to disclose information about ongoing affiliations with the PRC.
- Dr. Chen also allegedly failed to disclose a PRC bank account of >\$10K.

Source: DOJ Website: <https://www.justice.gov/usao-ma/pr/mit-professor-arrested-and-charged-grant-fraud>

Dr. Gang Chen: Conclusion

➤ Main Issues:

- Foreign Talent Program Participation (At least 2)
- Foreign Appointments (Various)
- Financial Conflict of Interest Disclosure (Received at least \$29 million)
- Conflict of Commitment Disclosure (Multiple foreign appointments)
- Other Support Disclosures (DOE/Other federal agencies)

➤ Consequences:

- Individual: All charges (wire fraud, foreign bank account filing, false tax return statement) were dropped in January of 2022.




Case Study Take Home Message

“He (Gang Chen) disclosed everything that he was supposed to disclose and never lied to the government or anyone else.”

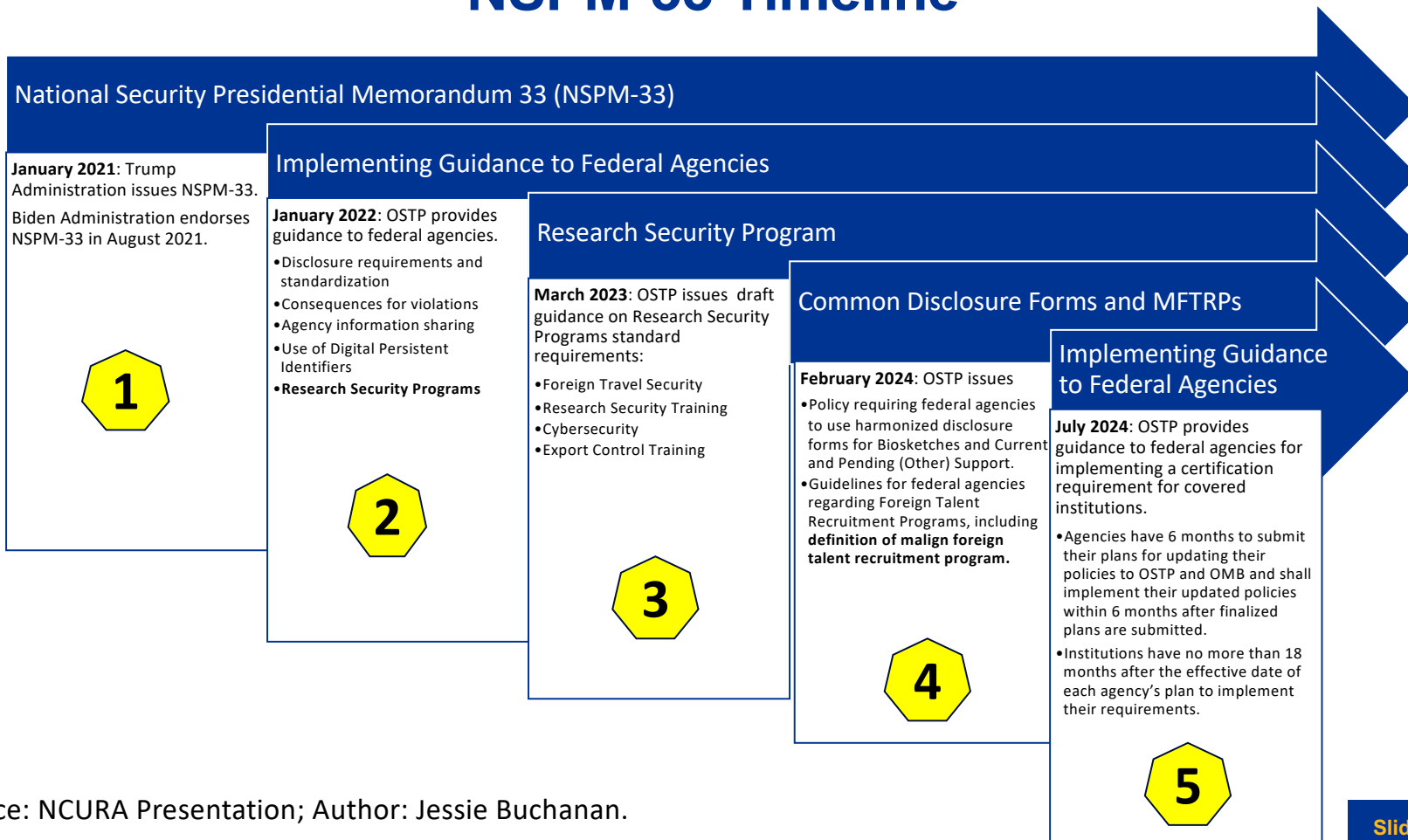
Robert Fisher, Dr. Gang Chen’s defense attorney

NSPM-33 & CHIPS

National Security Presidential Memorandum 33 (NSPM-33)

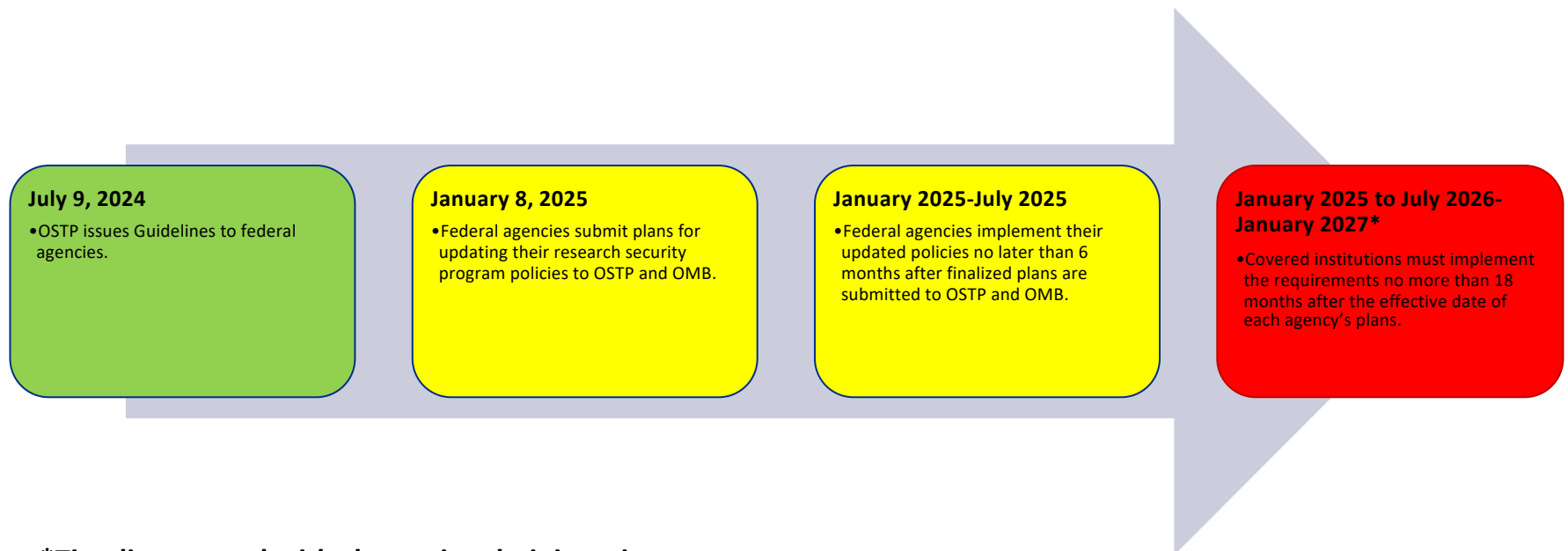
- **Established National Security Policy for the Research Enterprise** 
- **Topics Addressed:**
 - Enhanced Disclosure Requirements
 - Digital Persistent Identifiers
 - Standard Forms Across Federal Agencies
 - Continuation of HEA Section 117 Foreign Contract/Gift Reporting
 - Strengthened Penalties for Non-Disclosure
 - Secretary of State Reviews of Foreign Students and Researchers
 - Research Security Training
 - Research Security Programs for Institutions Receiving >\$50 M Federal Funding
 - Promote and Protect International R&D Cooperation

NSPM-33 Timeline



Source: NCURA Presentation; Author: Jessie Buchanan.

NSPM-33 Implementation Timeline



***Timeline paused with change in administration.**

See OSTP's July 2024 Guidelines Memo for definitions of "Covered institution", "Covered individual", etc.

Source: NCURA Presentation; Author: Jessie Buchanan.



NSPM-33: Research Security Requirements

- Treat everyone equally, without xenophobia, prejudice, or discrimination.
 - Do not target, stigmatize, or discriminate against individuals on the basis of race, ethnicity, or national origin.
- Covered Institutions (> \$50 million/year in federal support) must certify that they have implemented a research security program.
 - Certification will be via SAM.gov.
- Programs must contain four elements:
 1. Cybersecurity
 2. Foreign Travel Security
 3. Research Security Training
 4. Export Control Training
- Agencies can expand requirements.

Source: NCURA Presentation; Author: Jessie Buchanan.

NSPM-33: Required Elements of an RS Program



Cybersecurity

Implement a cybersecurity program consistent with NIST.



Foreign Travel Security

Periodic training (every 6 years)
Travel reporting program



Research Security Training

Implement a research security training program and ensure that covered individuals complete the training.



Export Controls Training

Provide training to relevant personnel on compliance with federal export control requirements and reviewing foreign sponsors, collaborators, and partnerships.

The following guidance is from the July 9, 2024, OSTP Guidelines for Research Security Programs at Covered Institutions.
Source: NCURA Presentation; Author: Jessie Buchanan.



CHIPS Act Research Security Sections

10337: Responsible
Conduct in Research
(RCR) Training

10338: Research
Security and Integrity
Information Sharing
Analysis Organization

10339A: NSF Funding
Restrictions to
Institutions Hosting
Confucius Institutes

10339B: Foreign
Financial Support

10631: Requirements
for Foreign Talent
Recruitment Programs

10632: Malign Foreign
Talent Recruitment
Program Prohibition

10633: Review of
Contracts and
Agreements

10634: Research
Security Training
Requirement for Federal
Research Award
Personnel

Rationalizing CHIPS & Science with NSPM-33

NSPM-33

- Disclosure of Foreign Gifts & Contracts (HEA Section 117)
- Foreign Talent Recruitment Programs
- Research Security Training

- Foreign Travel Security
- Cybersecurity
- Export Controls Training
- Other Support Disclosure Requirements



CHIPS

- Disclosure of Foreign Gifts & Contracts (NSF FFDR)
- Foreign Talent Recruitment Programs
- Research Security Training

- Responsible Conduct of Research Training
- Review of Contracts and Grants to Identify and Mitigate Risk

Source: NCURA Presentation; Author: Jessie Buchanan.

Current Implementation Status for Common Funding Agencies

Agency	Disclosures	Agency Risk Assessment	Conflict of Interest/Commitment	Training	Certification	Research Security Program
DARPA	●	●	●	Project specific	●	●
Defense	●	●	●	Project specific	●	●
Energy	●	●	●	●	●	●
NASA	●	●	●	●	●	●
NIH	●	●	●	●*	●	●
NSF	●	●	●	●	●	●

● Yes
● No/TBA

*NIH will require RS training for due dates => 05/25/2026.

Source: NCURA Presentation; Author: Jessie Buchanan.

Malign Foreign Talent Recruitment Programs

What is a Foreign Talent Recruitment Program?

Any program, position, or activity that includes:

- Compensation *to the individual* in the form of:
 - Cash
 - In-kind compensation, including:
 - Research funding
 - Promised future compensation
 - Complimentary foreign travel
 - Things of non de minimis value
 - Honorific titles
 - Career advancement opportunities
- Provided by:
 - A foreign country (any level of government) or their designee, or
 - An entity based in, funded by, or affiliated with a foreign country

Full definition found [in February 14, 2024 OSTP Memo](#) to Federal Research Agency Heads

What Makes a Foreign Talent Program “Malign”?

Compensation for:

- Unauthorized transfer of IP/research materials.
- Establishing a company or lab, accepting a faculty position, or undertaking other employment in violation of a federal award.
- Inability to terminate the arrangement.
- Required to apply for and receive R&D funds from the foreign government.
- Required to omit or alter acknowledgements in publications.
- Prohibited from disclosing the relationship to federal funding agencies or U.S. home institution.
- Requires a conflict of interest or conflict of commitment with institutional policies.

Question to Ask: Will the terms violate U.S. Research Integrity Principles?



AND

- A program that is sponsored by:
 - A foreign country of concern (currently China, Iran, North Korea, or Russia); or
 - An academic institution on the Department of Defense List of Concern (*1286 List)

*1286 List website location: https://rt.cto.mil/wp-content/uploads/2024/07/FY23-Lists-Published-in-Response-to-Section-1286-of-NDAA-2019_clearedv2.pdf.

FTRP Solicitation Example

From: Jason He
To: [REDACTED]
Subject: Check your talent project please 02/22/2024
Date: Wednesday, February 21, 2024 3:14:02 PM

Dear [REDACTED]

It is our great pleasure to welcome you to apply the **Qiming Talent Project**(Batch 4), Which is the china national top talent plan and no nationality limited.

On behalf of the local government ,We will assist you to complete the application throughout the process.

If you are selected, you will receive national talent honors, at least 2 millions financial support, world-leading work platform, and superior family living conditions. Certainly, for the requirement, you need to decide whether to accept it in three months, and you have to work full-time in China for at least 3 years. ~~The government reward will be implemented~~ after you sign a formal contract with the interested unit

Appliction conditions(no limit to nationality)

1. Ph.D;
2. Either of the following conditions:
 - Has held senior positions in foreign companies;
 - Serve as an associate professor or above in a foreign university or scientific research institution;

Also, you can forward this information to your friends who concerned.

Looking forward to your reply.

Warning Signs:

1. Funding comes from a local government in China.
2. Requires 100% effort for 3 years in China.
3. Applicants need to have a Ph.D. and history of leadership positions.



Things that are not Malign Programs

1. Making scholarly presentations and publishing written materials regarding scientific information not otherwise controlled under current law;
2. Participating 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;
3. Advising a foreign student enrolled at an institution of higher education or writing a recommendation for such a student, at such student's request;



Practical Considerations

- Federal Agencies are now prohibited from funding key personnel who are also participating in a Malign Foreign Talent Recruitment Programs.
- Federal R&D application rules now include the requirement that either/both the institution and key personnel certify that they are not participating in a MFTRP at the time of application submission.
- The only true way to identify a Malign Foreign Talent Recruitment Program is by examining the terms and conditions of the contract.
- ORSTC is available to review the terms of an outside employment contract only to determine whether it is an MFTRP.
- Additional information can be found on the ORSTC website:
<https://www.researchsecurity.pitt.edu/research-security/foreign-talent-recruitment-programs>.

Research Security Training



New Federal Agency Requirements

- The CHIPS Act section 1063 requires federal grant making agencies to establish research security training requirements for key personnel and their sponsoring institutions.
- DOE (05/01/25), NSF (10/10/25) and NIH (05/25/26) have all announced their deadlines for this training.
- DOD does not have a universal deadline for research security training but should check solicitations until agency-wide requirements are set.
- USDA research security requirements are dependent on the terms and conditions of the award.
- More information can be found on the ORSTC Website at:
<https://www.researchsecurity.pitt.edu/research-security/federal-research-security-training>.



University of Pittsburgh RS Training

- The University of Pittsburgh has adopted a consolidated version of research security training modules created under an award from the NSF.
- The consolidated research security training is managed through the CITI platform and can be accessed at: <https://www.citi.pitt.edu/>.
- The Office of Sponsored Programs verifies that all key personnel listed on an application to a federal agency having a stated RS training deadline have successfully completed this training module before an application is submitted.

Federal Agency Risk Reviews and Inquiries



Federal Risk Review Summary

- Section 10633 of the CHIPS Act provides authority to funding agencies to request supporting documentation for all key personnel on applications.
- Supporting documentation can be copies of federal and non-federal grants and contracts **AND PERSONAL OUTSIDE EMPLOYMENT DOCUMENTS**.
- The purpose of these reviews is to identify any existing activities that may overlap or interfere with proposed funding agency activities.
- Federal agencies have the ability to suspend or terminate an award if overlap or elevated risk is identified.
- Agencies can also request the development of a risk mitigation plan to manage higher risk activities.

DOD Policy on Risk Based Security Reviews

- Applies to FR awards selected for funding
- Driven by NSPM-33, NDAA 1286, CHIPS
- Review covers potential COI/COC
- List of mitigation steps for identified risk
- Appeals process is available
- New Risk Matrix included
- New published lists for MFTRPs and Chinese, Russian and other country “institutions” known to participate in illicit activities

[Link: Countering Unwanted Foreign Influence in Department-Funded Research at Institutions of Higher Education \(defense.gov\)](https://defense.gov)



Federal Agency Risk Perception

Risk	DOD	DOE	NSF	NIH
Academic appointments with universities in foreign countries of concerns	High	High	High	High
Direct funding from entities in foreign countries of concern	High	High	Med	High
Co-authored papers with collaborators affiliated with foreign countries of concern in the past 5 years	High	Med	Low	Med
Named collaborators from entities of concern	High	High	High	High



Examples of Risk Mitigation Measures

- Clarification of relationship.
 - Extent, timing, etc.
- Additional research security training.
- Prior notification of international travel.
 - Related or unrelated to the award.
 - **Includes personal travel in some cases.**
- Reporting suspicious inquiries.
- Concurrence from the sponsor on any planned international collaborations or co-authorships associated with the award.
- Discontinuation of certain international collaborations for the duration of the award.
- Ceasing certain associations or affiliations (both personally and institutionally).



What To Do When an Inquiry is Received

1. Don't Panic! Inquiries are becoming more common across academia.
2. Do **NOT** respond directly to the inquiry- OSP must respond back to the agency to confirm institutional endorsement.
3. Contact ORSTC or OSP if the federal agency sends the inquiry directly to the PI, department or school.
4. ORSTC will identify the specific agency concerns and discuss with the PI or affected Pitt key personnel.
5. ORSTC will draft a risk mitigation plan/official response and review with the PI or affected Pitt key personnel.
6. Once the PI/key personnel and ORSTC have agreed on the plan, ORSTC will provide it to OSP who will submit it to the agency.

Cybersecurity



NSPM-33 Cybersecurity Rule

From 07/09/2024 OSTP Memo For the Heads of Federal Research Agencies

- “As the first element of the standardized requirement, federal research agencies shall require institutions of higher education to certify that the 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.”
- “For covered institutions that are not institutions of higher education, federal research agencies shall require covered institutions to certify that the institution will implement a cybersecurity program consistent with another relevant cybersecurity resource maintained by NIST or another federal research agency.”

Source: ASCE Presentation



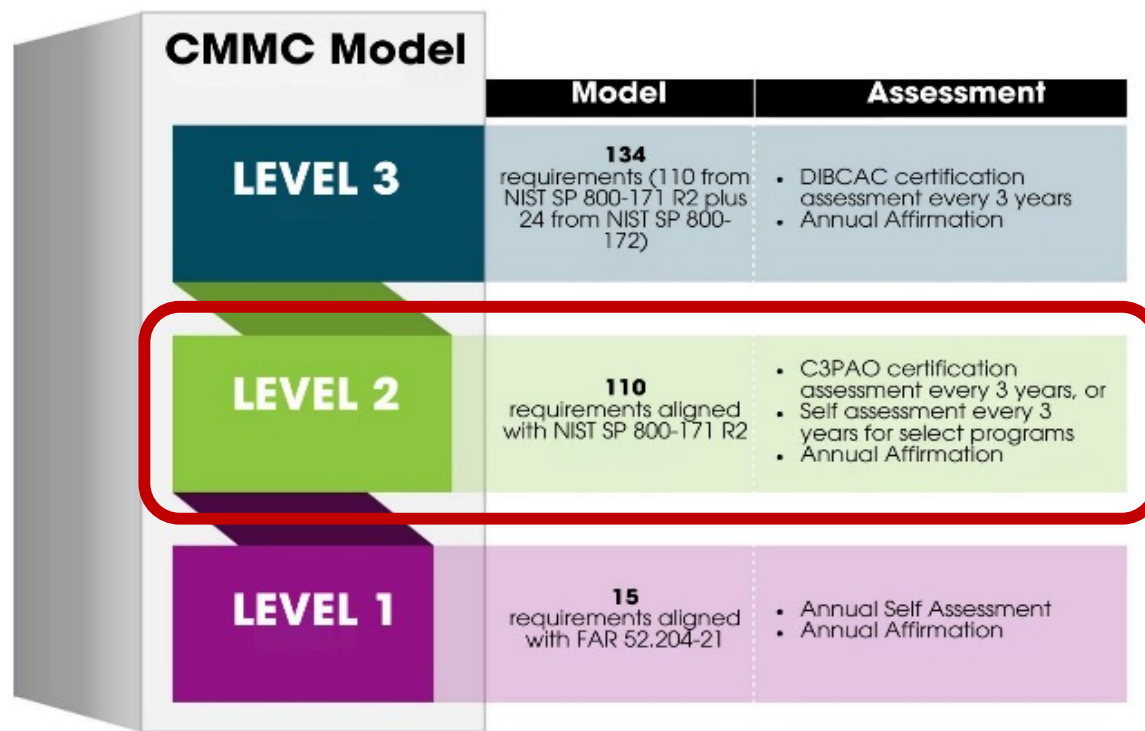
While We Wait...There are Some Clues

- **Similar Baseline Cybersecurity Requirements Currently Appear in:**
 - Recent FDP Demonstration Cybersecurity Framework.
 - NSTC Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33)
 - FAR Clause 52.204-21 “Basic Safeguarding of Covered Contractor Information Systems”
 - DOD Cybersecurity Maturity Model Certification (CMMC) Level 1
- **Programs that Require Enhanced Cybersecurity Requirements through NIST SP 800-171**
 - Controlled Unclassified Information (CUI) Program Rules
 - DOD Cybersecurity Maturity Model Certification (CMMC) Level 2
 - NIH Controlled Access Genomic Data

NSPM-33 Requirements (From 2022 Implementation Guidance)

System access	Network connectivity	Malicious code	Other
<ul style="list-style-type: none">• Control system access by user, device (#1)• Control system access to transactions, functions (#2)• Identify accounts acting on behalf of users, devices (#5)• Verify identities of user accounts (#6)	<ul style="list-style-type: none">• Control connections to and use of external systems (#3)• Monitor, control network connections (#7)• Separate network connections for public systems (#8)	<ul style="list-style-type: none">• Protect from malicious code, software (#10)• Update malicious code protections timely (#11)• Scan systems and files for malicious code (#12)	<ul style="list-style-type: none">• Control non-public on public systems (#4)• Correct system flaws, vulnerabilities timely (#9)

DOD's CMMC Program



- Pitt Digital and ORSTC are working to achieve C3PAO certification for CMMC Level 2.
- It is anticipated that this environment will be operational by Spring 2026.
- In the interim, the University does not have a compliant NIST 800-171 environment to safeguard controlled unclassified Information.



Cybersecurity Summary Comments

- According to University Policy RI 14 Research Data Management, research records must be stored in University owned or controlled or approved resources, facilities, or repositories.
- Until NSPM-33 is fully implemented, federal grant terms and conditions allow institutions to determine cybersecurity around open research results.
- Federal contract terms and conditions typically define cybersecurity requirements through FAR and DFAR clauses.
- OSP circulates awards containing Cybersecurity terms and conditions that require enhanced protections to Pitt Digital and ORSTC for review and follow-up with other central offices or the PI in many cases.
- Please reach out to ORST with any questions around CUI or CMMC:
<https://www.researchsecurity.pitt.edu/research-security/controlled-unclassified-information-cui>.

Topics on our Radar



Summary of RS Developing Topics

- Export Controls and how they overlap with Research Security (Future webinar being planned)
- NIH Policy on Enhancing Security Measures for Human Biospecimens, <https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-160.html>.
- DOJ Bulk Sensitive Data Rule, https://researchservices.upenn.edu/wp-content/uploads/2025/08/data_security_program_cheat_sheet.pdf.
- NIH Policy on Enhancing Security Measures for NIH Controlled-Access Data, <https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-083.html>.



Office of Research Protections, Research Security and Trade Compliance

THANK YOU!

[Researchsecurity.pitt.edu](https://researchsecurity.pitt.edu)