



National Security Presidential Memorandum-33: Best Practices and Lessons Learned

National Council of University Research Administrators

February 13, 2023

© 2023 National Council of University Research Administrators

Today's Agenda



Research Security Refresher and Status Update

- Research security timeline
- Status of NSPM-33 Implementation Guidance efforts
- CHIPS-plus-Science Act

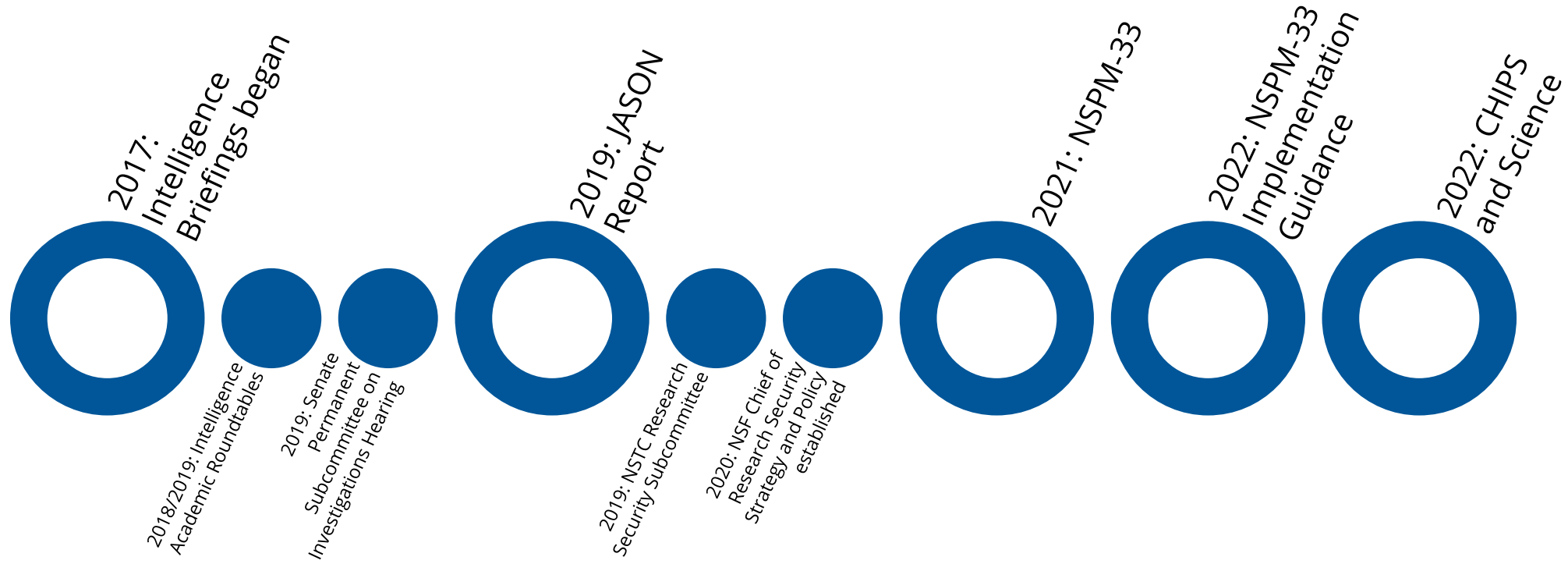
Institutional Perspectives

- History
- Research security programs requirements and institutional approaches to address them

Research Security Training Modules

Institutional staffing and infrastructure for addressing research security requirements

Research Security Timeline



Status of NSPM-33 Implementation Guidance Efforts

- Harmonized disclosure formats
- Research security training modules
- Research security program standards
- Digital Persistent Identifiers



CHIPS-plus-Science Act, Passed in August 2022

Several research security provisions including:

- Prohibition of malign foreign talent recruitment programs for federally funded researchers
- Requirement for NSF to establish a Research Security and Integrity Information Sharing and Analysis Organization
- Research security training requirement for all covered personnel on federal awards
- Inclusion of research security training as part of Responsible and Ethical Conduct of Research training
- Reporting (to NSF) on foreign financial transactions and gifts above \$50,000 associated with countries of concern
- Prohibition of Confucius Institutes



Institutional Perspective – How did we get here?

Aug. 2018 NIH Letters



Jan. 2021-22 NSPM-33 & Guidance



CHIPS-plus-SCIENCE Act



Sept. 2022 Common Forms



2023 Expected Guidance

In the news...

U.S. Drops Its Case Against M.I.T. Scientist Accused of Hiding China Links

Gang Chen, a professor of mechanical engineering, was arrested a year ago, accused of concealing his affiliations with Chinese government institutions.

NEWS | 07 March 2022

'I lost two years of my life': US scientist falsely accused of hiding ties to China speaks out

Acquitted nanotechnology researcher Anming Hu returns to his lab after two years – and is still grappling with the aftershocks of his ordeal.

Department of Justice

U.S. Attorney's Office

District of Massachusetts

SHARE 

FOR IMMEDIATE RELEASE

Tuesday, December 21, 2021

Harvard University Professor Convicted of Making False Statements and Tax Offenses

Dr. Charles Lieber found guilty of concealing his affiliation with the Wuhan University of Technology and his participation in China's Thousand Talents Program

Probation, Not Prison, for Researcher in China Initiative Case

A jury convicted the former chemical engineering professor on charges linked to allegedly failing to disclose ties to China, but a judge threw out several of the convictions and imposed the lightest possible sentence.

By **Jaime Adame** • Published January 20, 2023

How does undue foreign influence manifest?

Violating confidential peer review process

- Manuscripts
- Proposal applications

Taking IP from the US and filing patents outside the US

Undisclosed appointment/affiliations/funding that duplicate US federal funding and/or effort

- Foreign talent programs
- Appointments at other institutions
- Other support (grants, funded staff, consulting) that overlaps federal effort/funding

Research Security Programs

Required for institutions that receive over \$50M in Federal R&D funding annually



Includes

Cybersecurity

Foreign Travel Security

Research Security Training

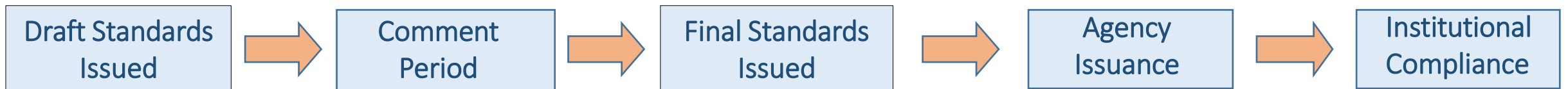
Export Control Training



Implementation details expected in 2023

Research Security Program *Timeline*

- OSTP, in consultation with the NSTC Subcommittee on Research Security, OMB, and external stakeholders, will develop a standardized requirement for uniform implementation across research agencies.
 - Draft standard requirements for research security programs and a certification process.
- Following a 90-day comment period, OSTP will complete the requirements in the subsequent 120 days, and, upon completion, work with OMB to develop an implementation plan.
- Upon receipt of the standards, relevant research agencies should engage with external stakeholders to ensure that program requirements are appropriate to the broad range of organizations subject to them.
- **From the time individual *agency guidance* is issued, institutions will have one year to come into compliance.**



Research Security Program *Documentation Requirements*

- Research organizations are required to maintain a description of the research security program, and to provide such documentation within 30 days of a request from a research agency that is funding an R&D award or considering an application for R&D award funding to that research organization.
 - Institutions can begin documenting existing policies and processes relative to the information available in the NSPM-33 implementation guidance and identifying gaps
- Research organizations should be provided flexibility to structure the organization's research security program to best serve its particular needs, and to leverage existing programs and activities where relevant.

RSP Requirements: Cybersecurity

- Requires compliance with 12 of the 15 requirements of FAR 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems* and 2 additional requirements (cybersecurity awareness training and protection of scientific data from ransomware - 14 total requirements).
- Additional cybersecurity requirements will apply in some cases, such as for research involving classified or controlled unclassified information.



RSP Requirements: Cybersecurity

- Institutional assessment, centrally and at individual schools and centers:
 - Current status and planned efforts relative to the requirements
 - Anticipated challenges for implementation
 - Potential impact on faculty, staff, and students and how to reduce negative impact
 - Estimated costs
 - Estimated timeline for implementation
 - Additional considerations



RSP Requirements: Foreign Travel Security



- Maintain international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, research purposes, or any offers of sponsored travel that would put a person at risk.
 - Discussed this language during an OSTP listening session – Staff on a federal award? Additional guidance on “would put a person at risk”?
- Such policies should include an organizational record of covered international travel by faculty and staff and, as appropriate, a disclosure and authorization requirement in advance of international travel
 - Document institutional policies and processes that address this requirement as part of the research security program.

RSP Requirements: Foreign Travel Security



- Such policies should include an organizational record of covered international travel by faculty and staff and, as appropriate, a disclosure and authorization requirement in advance of international travel – Cont.
 - Some institutions required registration of international travel during the pandemic, with record retention, and retained this.
 - Ensuring faculty and staff understand and comply with policy. To what extent can it be automated? Challenge of travel reimbursed by an outside entity. (Incentives, e.g., international travel insurance)
 - Work with appropriate institutional staff to identify and address any gaps
- Security briefings, assistance with electronic device security (smartphones, laptops, etc.), and pre-registration requirements.
 - Document policies and processes and identify and address gaps. Consideration of resources.

RSP Requirements: Training

Research Security Training

- Research organizations provide training to relevant personnel on research security threat awareness and identification, including insider threat training where applicable.
- NSF, NIH, DoD and DoE funded four cooperative agreements for the “development and implementation of training to recipients of federal research funding in best practices to optimize research security.”
- Training modules should be available by the end of 2023 for institutions to adapt and use.
 - Why is research security an important issue?
 - What is a disclosure policy and how will it be used?
 - What actions can federally funded research recipients take to manage and mitigate risk?
 - Is international collaboration encouraged?

RSP Requirements: Training

- Development of learning objectives and content is underway for the four modules, with content being developed collaboratively with agency representatives.
- The teams came together and met with federal staff on February 6 and will continue to engage and collaborate.
- Modules are anticipated to have multiple tracks, including for research administrators with effective practices for implementing a research security program.
- Focus groups are currently underway for the Risk Management and Mitigation Module.
 - 8-9 sessions, ~100 participants: 45 PIs/Senior Personnel, 20 graduate students/post-docs, 24 research administrators, 11 senior research officers
- Module design and development is the next major phase, followed by pilot testing.

RSP Requirements: Training

CHIPS and Science Act Section 10337, Responsible Conduct in Research Training

- Expands training to faculty and other senior personnel
- Expands the scope of training to include “...training to raise awareness of research security risks as well as Federal export control, disclosure, and reporting requirements.”
 - Will the latter requirement be implemented after the research security training modules are completed?
 - How long will institutions have to incorporate the training modules, or aspects of them, into RCR training?

RSP Requirements: Training

Export Control Training

- Require that *research organizations conducting R&D subject to export control restrictions* provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and ensuring compliance with Federal export control requirements and restricted entities lists.
 - Assess and document current institutional training.

Cybersecurity Training

- Assess and document current institutional training.



University of Arizona Inventory

■ Foreign Travel

- Current process for pre-travel authorization
- Long-standing committee to evaluate foreign travel – evaluate procedures
- Existing contracts to provide safety briefings

Intersects with:

- Export control

■ Export Controls



■ Training needs

- Evaluate all offerings for content
- RCR team on standby

Disclosure Lifecycle

Proposal/Preaward: Activities on appointments, collaborations, support

COI/COC: Significant financial interest and outside activities

Award: Change or hold award based on agency assessment of risk

Post-award: new or changed information, progress reports

Publication: Disclosure of support and possible conflicts, affiliations

University of Arizona Inventory

▪ Disclosures

- Conflict of Interest
- Conflict of Commitment

Intersect with:

- Proposal Applications
- Publications & Scholarly products

• Cybersecurity

- Compliance with standards
- Evaluate current training & tools

Intersect with:

- Impact to faculty working on CUI-covered research
- Insider threat training for new scenarios

Policies & Procedures Inventory

■ Research Office

- Conflict of Interest & Commitment
- Export Control
- Proposal application submission review
- JIT processes
- Progress Reporting

■ Campus Wide

- Cyber & Information Security
- Traveling with electronic devices
- Foreign Travel
- Risk Management

What's missing? Do you need to add new policies? Strengthen existing ones?

NSPM-33 – Persistent Identifiers

National Security Presidential Memorandum 33 Implementation Guidance

- Issued January 4, 2022. Directs federal research funding agencies to:
 - Incorporate persistent identifiers (PIDs) into their electronic systems and grant and cooperative agreement application and disclosure processes
 - Agency integration into grant management systems and SciENcv
 - Agencies *may require* PIDs as NIH has for research training, fellowship, education, and career development awards since FY2020
 - ORCID is the PID for individuals/researchers that meets federal requirements (e.g., non-proprietary).
 - Some agencies, such as NSF, will specify use of ORCID.
 - Allow, not require, submission of disclosure information via a PID service
 - Researchers can choose whether to make information available through their PID profile/record, such as ORCID.

NSPM-33 – Persistent Identifiers

The August 25, 2022, OSTP policy, [Ensuring Free, Immediate, and Equitable Access to Federally Funded Research](#) directs federal agencies to:

- **Instruct federally funded researchers to obtain a persistent identifier per the NSPM-33 Implementation Guidance, include it in published research outputs, and provide federal agencies with the metadata associated with all published research outputs they produce, consistent with the law, privacy, and security considerations.**
- **Assign unique persistent identifiers to all scientific research and development awards and intramural research protocols that have appropriate metadata linking the funding agency and their awardees through their digital persistent identifiers.**

Digital Persistent Identifiers (DPIs) or PIDs

- What is a DPI?
- What is a PID?
 - Unique
 - Findable
 - Machine Readable
 - Permanent
 - Unambiguous

Source:

<https://guides.library.vcu.edu/pids>

DOI
Digital objects or object metadata.
Exs: articles, eBooks, datasets

Grant ID
Identifies what supported a study
with either direct funding + other support

ROR
Research organizations
Universities, centers, partnerships,
research hospitals, and other organizations

RRID
Research Resources ID
Key biologicals and chemicals

ORCID
Researchers and future researchers

Funder Registry
Research funding source

A BETTER RESEARCH WEB
6 key PIDs to use when publishing

All images used by license from the Noun Project <https://thenounproject.com/>

NSPM-33 DPI standards


- Open, non-proprietary, researcher-driven
- Provided at no cost to the researcher
- Disambiguates one researcher from another (i.e., John Smith at U. Michigan and John Smith at U. Arizona)
- Allows trusted parties to write to PID records
- Allows integration of data to reduce researcher burden



Reducing Administrative Burden

- Information maintained in ORCID records can be accessed by research funders, publishers, institutions, and others at researchers' discretion
 - Work history, education, affiliations, funding awards, publications, data sets and other information that can auto-populate grant proposals and other forms.
 - Allow trusted organizations (e.g., NIH and home institutions) to access and add research information in ORCID records. Facilitates interoperability and data sharing between systems and workflows.
 - Allows research sponsors to pre-populate proposals and other forms with information in ORCID profiles (e.g., CV, biosketch, current and pending support)
 - NIH and NSF already allow researchers to import data from ORCID into SciENcv for Biosketches and will do the same for current and pending support.
 - Reduces initial and duplicative data entry with trusted organizations

Most recent NSF PAPPG: SciENcv
usage is encouraged; will be
required in October 2023



Integration with ORCID

Create NIH & NSF
Biographical Sketches

SciENcv team is prepping
for new common forms

Persistent Identifiers – Institutional Approaches

- Integration into grant management and other systems
- Educational initiatives and opportunities to create an ORCID and affiliate with home institutions
 - Highlight NSPM-33 requirements and associated federal efforts in webinars and resources
 - Identification of faculty, staff and trainees on federal awards
 - Providing personalized links to create an ORCID and/or affiliate home institutions with researcher's ORCID accounts – **Make it easy!**
- ORCID membership – ability to read and write to ORCID profiles through institutional affiliation and system integration

The logo for ORCID, with the letters 'ORCID' in a sans-serif font. The 'i' is lowercase and colored green, while the other letters are grey.

Connecting Research
and Researchers

University of Arizona

Develop
ORCID
strategy that
encompasses:

- Research Security (proposal application preparation)
- Bibliometric data sources
- Enterprise grants system (external and internal funds)

Broader
implications:

- Faculty Activity Reporting (P&T)
- COI/COC disclosures
- Data Management & Sharing/Public Access

ORCID Strategy

Is your institution an ORCID member?

How are you using your membership/how could you be using it?

How will you communicate the use of persistent identifiers?

Do your systems (eRA, etc.) capture an ORCID iD? Should they?

Who needs to know? Be Involved? Manages Compliance?



What are institutions doing?



Reorganizing offices / reporting lines



Hiring Research Security staff (Directors, Officers, Analysts)



Forming steering/governing committees



Socializing the idea on campus



Waiting to make big decisions

Common Approaches

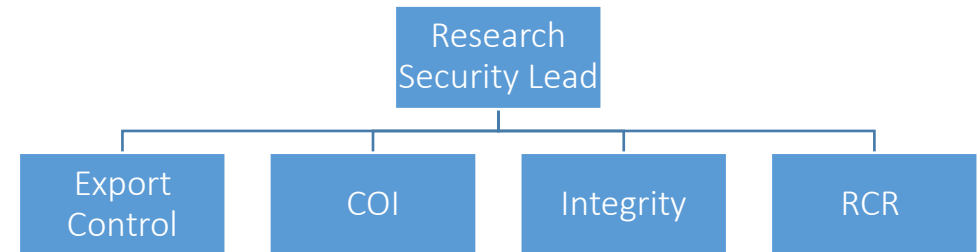
Coordination/Working Group

- No single area of direct authority over involved units
- Working group chair may/may not be Research Security lead



Institution Reorganization

- Research Security lead has direct oversight of some involved units



University of Arizona

■ Holistic Approach

- Steering/Operational committee made up of affected units
- Planned Research Security office
 - Executive Director TBH, Case Managers, Training Development & Support
 - Lifecycle analysis of foreign collaborations & reporting
 - Data analysis & technology support
- ED position will not manage other compliance functions (Export Control, COI, RCR) or pre-award proposal teams
- Goal: Proactive Faculty support
- <https://research.arizona.edu/compliance/research-security-hub>

Administrative Structure

- Coordination across the institution
 - Coordinating committee made up of affected units
 - Fosters communication and harmonization across the institution
 - Subcommittees and working groups address target areas specific to their unit (e.g., cybersecurity, disclosure, travel security)
 - Minimize administrative burden
- Executive Director position manages other compliance functions (e.g., Export Controls, research information security/CUI, COI)
 - Reduce silos in addressing research security and allow for holistic approaches (e.g., cybersecurity, outreach and other areas)
- Facilitating International Engagement
 - Providing information and tools to foster collaborations

Poll: How is your institution organizing around research security?

Research Security is rooted in:

- A. Sponsored Programs
- B. Conflict of Interest
- C. Export Controls
- D. A research security individual or office with oversight of one or more of these areas?
- E. All of the above

AGAIN: Who needs to know? Be Involved? Manages Compliance?



Recommendations

Identify who needs to know

Inventory of policies/procedures

Identify gaps

ORCID strategy

SciENcv usage

Ideas for reducing burden

What are the challenges?

- An evolving landscape with respect to international relations and associated policy requirements
- Federal forms and guidance are pending, and the extent of agency adoption and deviation is not known
 - Deviation should not be taken lightly
- Decentralized environments can result in different levels of risk assessment and mitigation across an institution.
- We don't know what we don't know
- Information lives in different places, on and off campus
 - Institutional Profile pages/department websites
 - Wikipedia
 - Where else?
- Do the right people have access to campus systems at the right time?

From your perspective, what are the greatest challenges for your institution? For researchers?

Join us for After the Show to share!

What is your institution doing, or can it do, to reduce administrative burden?

What resources is your institution providing researchers to:

- Enhance compliance
- Foster principled, reciprocal collaborations

**Join us for After
the Show to
share!**

