

P5 Conflict of Interest, NSPM-33, CHIPS, and DPI: Implications for Your Research Compliance Program

SCCE Higher Education
Compliance Conference

1	Introductions
2	Background and major cases
3	Changes to FCOI disclosures, grant applications, and DPI's
4	How to prepare now for what lies ahead
5	Questions



Amanda Ferguson

Sr. Director

Huron Consulting Group
aferguson@hcg.com



Rebecca Scott

Sr. Associate

Huron Consulting Group
rscott@hcg.com

Recent policy
and practice-
related
background



Polling Question #1

Which description best fits the state of your institution's research security program (RSP) implementation?

1. Not started.
2. Initial planning stages (NSPM-33 gap analysis and readiness assessment).
3. Implementation has begun, but is in its infancy.
3. Nearly complete with implementation.
4. Program established, but continuing to refine approach.

Overview and Background

A timeline of key regulatory updates.



NOV 2018

DOJ China Initiative Launch

Strategic initiative to counter Chinese national security threats specifically; citing that China was involved in 60% of all trade theft cases.

JUL/AUG 2019

NIH/NSF Dear Colleague Letters

Both agencies issued letters reminding grantees and the research community of the values of openness, transparency, and reciprocal collaboration in response to concerns.

JAN 2019

DOE Memo RE: Talent Programs

DOE issues memo prohibiting participation in foreign talent recruitment programs for recipients of financial assistance.

AUG 2021

Biden Administration: Clear Rules for Research Security and Researcher Responsibility

Biden OSTP reaffirms commitment to NSPM-33.

JAN 2021

Trump Administration: NSPM- 33

Trump OSTP announces NSPM-33, directive to US Gov't R&D to strengthen protections for intellectual capital and discourage research misappropriation.

JUL 2019

NIH "Other Support" Guidance

NIH issued a notice reminding awardees and researchers of policies related to Other Support and Financial Conflicts of Interest.

JAN - AUG 2022

NSPM-33 Implementation Guidance and Updates Released

Biden OSTP releases initial implementation guidance and subsequent updates.

JAN 2023

NSF PAPPG updates and National Counterintelligence and Security Center toolkit

Federal government begins to operationalize NSPM-33.

MAR 2023

OSTP seeks comments on Research Security Programs Standard Requirement

Would like to ensure uniformity across federal agencies when developing requirements.

Overview and Background

From 2017 – mid 2021, the enforcement actions were so frequent that keeping up was difficult.

MD Anderson



2017 - 2018

- NIH contacted cancer center regarding 5 researchers in 2018 (FBI involved since 2017).
- One researcher violated peer review confidentiality by emailing an NIH award application to a Chinese scientist; others had undisclosed appts., affiliations, or COIs.
- Two researchers resigned and a third was fired.

Van Andel Research Institute



December 2019 and September 2021

- *\$5.5M settlement in 2019: Accused of violating the False Claims Act by knowingly submitting federal grant applications/RPPRs which failed to disclose Chinese gov't funding.*
- *\$1.1M settlement in 2021: for failing to disclose a foreign component.*

Harvard University



January 2020

- Chair of chemistry and chemical biology department arrested and charged with making false statements to federal authorities about participation in a Chinese talent program, plus tax and foreign bank account-related counts.
- Admitted in a taped FBI interview to transporting cash from China to Boston totaling \$50-100K.
- Found guilty of all charges in 2021; sentenced in April 2023.

Emory University



May 2020

- NIH reviewed faculty member's grant applications and suspected undisclosed foreign research activity.
- DOJ found investigator had earned \$500,000 in income between 2012 – 2018 that was never reported.
- Faculty member pleaded guilty to filing a false tax return; sentenced to probation and ordered to pay restitution.

West Virginia University



August 2020

- Faculty member submitted fraudulent request for alternate work/parental leave in Fall 2018; worked in China for Chinese Academy of Sciences – received living subsidy (\$143k), research subsidy (\$573k), and salary (\$87k).
- Pled guilty to 'federal program fraud' for undisclosed participation in 1,000 talents program.
- Sentenced to three months in prison and ordered to pay restitution.

MIT



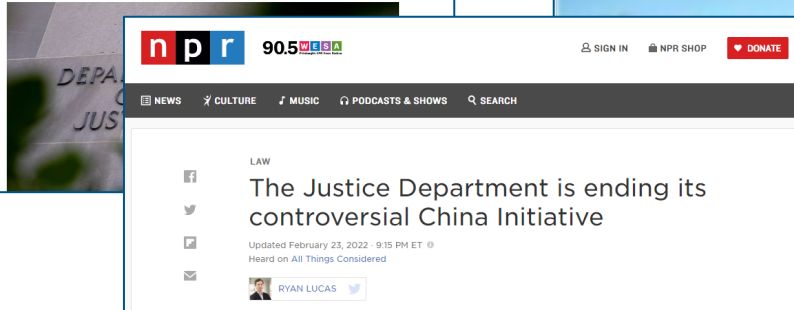
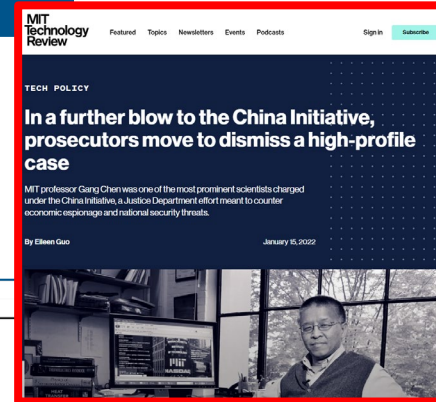
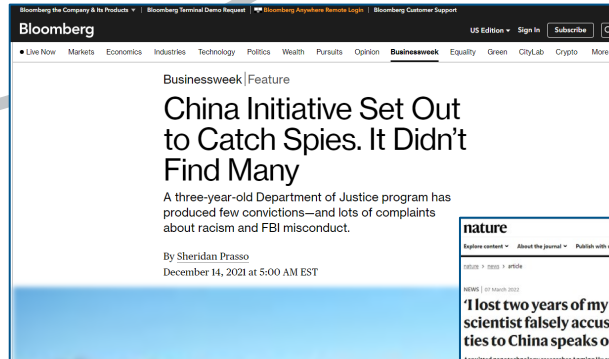
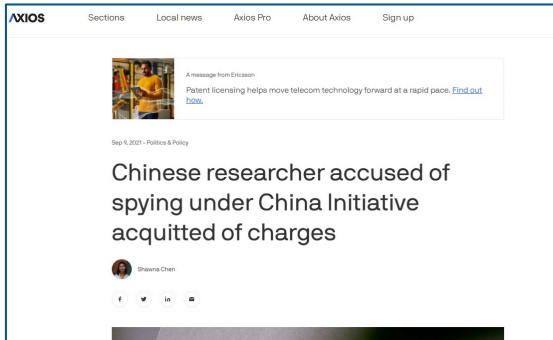
January 2021

- Faculty member arrested/charged with wire fraud, failing to report a foreign bank account, and making false statements in a tax return.
- Allegedly failed to disclose participation in two talent programs; received \$29M in foreign funding, \$19M from PRC, while also receiving U.S. federal grant money.
- Case dismissed at DOJ's request in January 2022.

Overview and Background



The DOJ's China Initiative was sunset in early 2022, in part due to criticism that it was ineffective and inconsistently pursued, and in part due to some instances of FBI misconduct. Some cases were thrown out, and some of the accused were acquitted.

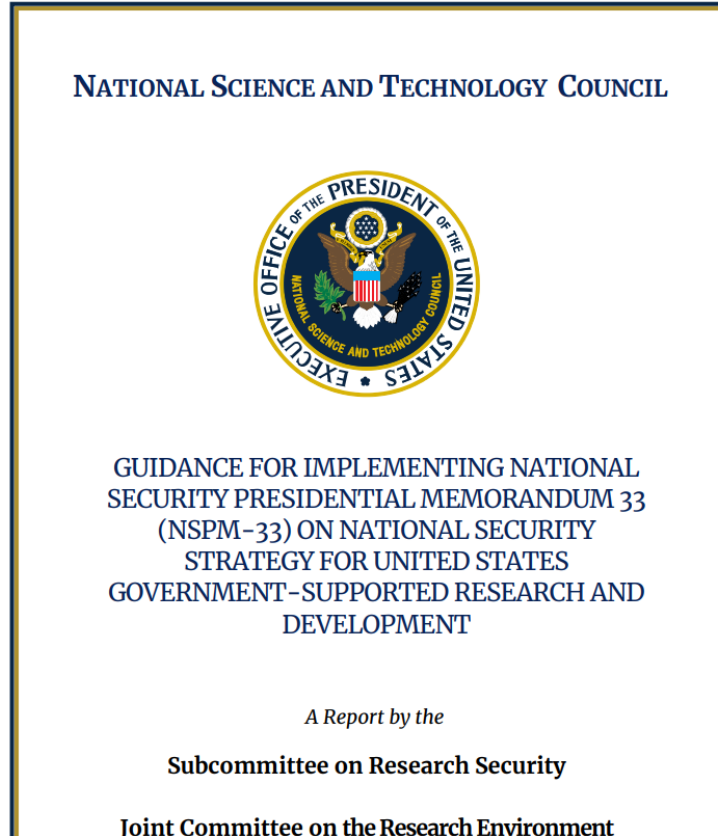


Enforcement Update

Major case updates from highly publicized cases

Harvard	MIT	Kansas	Tennessee	Ohio State
<ul style="list-style-type: none">• Prof. Charles Lieber found guilty on all charges in December 2021.• Retired from Harvard in February 2023.• Agreed to pay ~\$34K in restitution in advance of sentencing.• Sentenced in April 2023 to time served (~2 days of incarceration), 2 years of supervised release, of which 6 months will be home confinement, and a \$50,000 fine.• Remains suspended from conducting federally funded research per SAM database.• Civil case against Harvard seeking indemnification for legal fees remains ongoing.	<ul style="list-style-type: none">• DOJ abandoned its criminal case against Prof. Gang Chen in January 2022, citing an inability to meet the burden of proof.• USAO took the unusual step of holding a press conference to announce that the case was being dismissed.	<ul style="list-style-type: none">• Prof. Franklin Tao accused of failing to disclose participation in Chinese talent program.• DOE and NSF representatives testified at trial that they were satisfied with Prof. Tao's work.• Convicted of one false statement and three wire fraud counts.• In September 2022, the Court granted Prof. Tao's motion for acquittal on the wire fraud counts.• Sentenced to time served for false statement conviction.• Appeal pending as of late May.	<ul style="list-style-type: none">• Prof. Anming Hu accused of intentionally hiding ties to a Chinese university while performing work for NASA.• Charged with three counts each of wire fraud and making false statements.• Mistrial in June 2021 after the jury could not reach a verdict.• Court granted motion for judgment of acquittal, denying DOJ the opportunity to retry the case; opinion stated in part that NASA got the work it bargained for.	<ul style="list-style-type: none">• Entered into a November 2022 settlement with DOJ to resolve civil allegations that it failed to disclose a researcher's employment at a foreign university, participation in a talent program, and foreign grant.• Paid \$867K and agreed to cooperate with the government's investigation.

Issued in January 2022, updated in October 2022, and talked about ever since.



Polling Question #2

Which description best describes your familiarity with NSPM-33 and CHIPs?

1. I know it by heart.
2. I've generally read it.
3. My institution has some people working on it.
4. Nearly complete with implementation.
5. I have no idea what that is.

NSPM-33

General Summary

- On Jan. 4, 2022, the White House Office of Science and Technology Policy (OSTP) published a blog [post](#) announcing OSTP’s release of [guidance](#) to federal agencies toward implementing National Security Presidential Memorandum 33 (NSPM-33), which set forth national security strategy and principles for strengthening the protections of U.S.-funded research and development against foreign interference and exploitation.
- The post and the guidance directed federal research agencies to spend the next 120 days developing a set of model grant forms that can be used uniformly by researchers across funding agencies.



NSPM-33

Major points of guidance include:

- Federal funding agencies are directed to develop a model proposal disclosure form and instructions to promote the consistency of what researchers are expected to disclose and to allow researchers to report information in the same way, regardless of funding agency.
- Researchers must disclose detailed information about current and pending support, including:
 - Applications to programs sponsored by foreign governments, including foreign government-sponsored talent recruitment programs.
 - In-kind contributions.
 - Visiting scholars, students, and postdocs not paid by the researcher's institution.
 - Sponsored travel when performing research activities with an associated time commitment.
- Administrative remedies or enforcement against institutions are limited to three discrete scenarios.
- Institutions receiving more than \$50 million annually in federal research and development funding must establish and maintain research security programs that meet the implementation guidance's standards.

NSPM-33 Implementation Guidance was officially released in January 2022.

Consequences for researchers and institutions

- Outlined scenarios which require institutions to be held accountable and update business processes, & policies.
- Established mandatory reporting thresholds.
- Requires faculty to understand they have personal liability and responsibilities.

Research Security Programs

- Mandates that institutions who receive >\$50M annually to establish research security programs.

Standard disclosure requirements for applicants

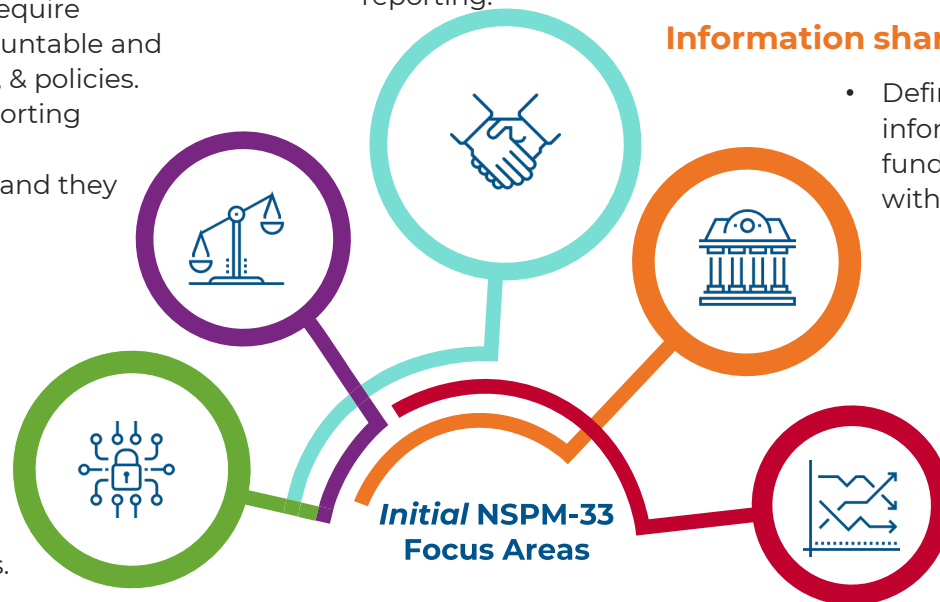
- Established disclosure requirements, requiring institutional COI/COC programs to ensure content of disclosures are aligned with anticipated requirements.
- Delineated impacts to business processes across the award life cycle facilitate appropriate institutional review, submission, and mandatory reporting.

Information sharing among federal agencies

- Defines a government wide approach to information sharing among federal funding and enforcement agencies and with the public.

Digital Persistent Identifiers (DPIs)

- Requires the use of DPIs
- Full implementation of DPIs is still pending.



Policy Updates: OSTP Implementation Status

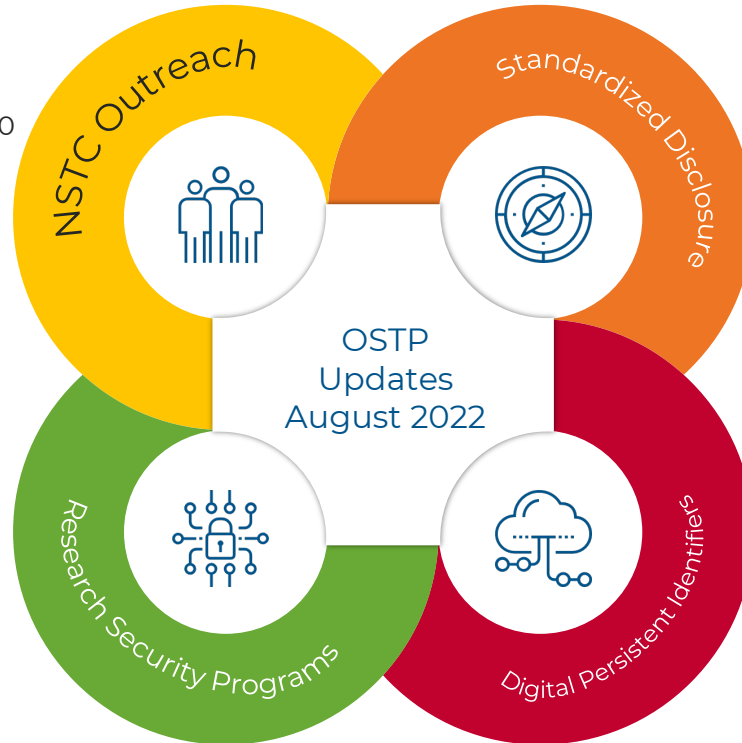
OSTP released an update on the status of NSPM-33 implementation in September 2022.

NSTC Outreach

- The Subcommittee on Research Security (SRS) has met with nearly 40 organizations about the NSPM-33 proposed requirements.
- Outreach is ongoing, and the SRS is seeking input from minority-serving institutions, rural institutions, and regional or community colleges.

Research Security Programs

- The CHIPS and Science Act extends the requirements for research security training to all covered individuals applying for federal science and engineering funding.



Draft Standardized Disclosure Requirements

- The NSF piloted standardized biographical sketch and current and pending (other) support forms.
- In-kind support that is directly related to the proposed project will be disclosed in Facilities, Equipment, and Other Resources, while similar support not directly related will be disclosed as Other Support.

Digital Persistent Identifiers

- The NSF disclosure requires use of ORCID (Open Researcher and Contributor ID) for all senior/key personnel.
- Product persistent identifiers are also required for all products listed in the Biosketch.

While it has been widely reported in the press that the China Initiative is “over,” the government’s interest in research security remains.

Remember:

- The People's Republic of China is only one of several countries of interest/concern.
- While DOJ has stepped back absent unusual circumstances, NIH, NSF, and DOD inquiries persist.

The current focus has expanded to include several countries of concern, and has centered around these key principles:

1. Avoiding wrongful IP transfers and preserving U.S. rights to inventions.

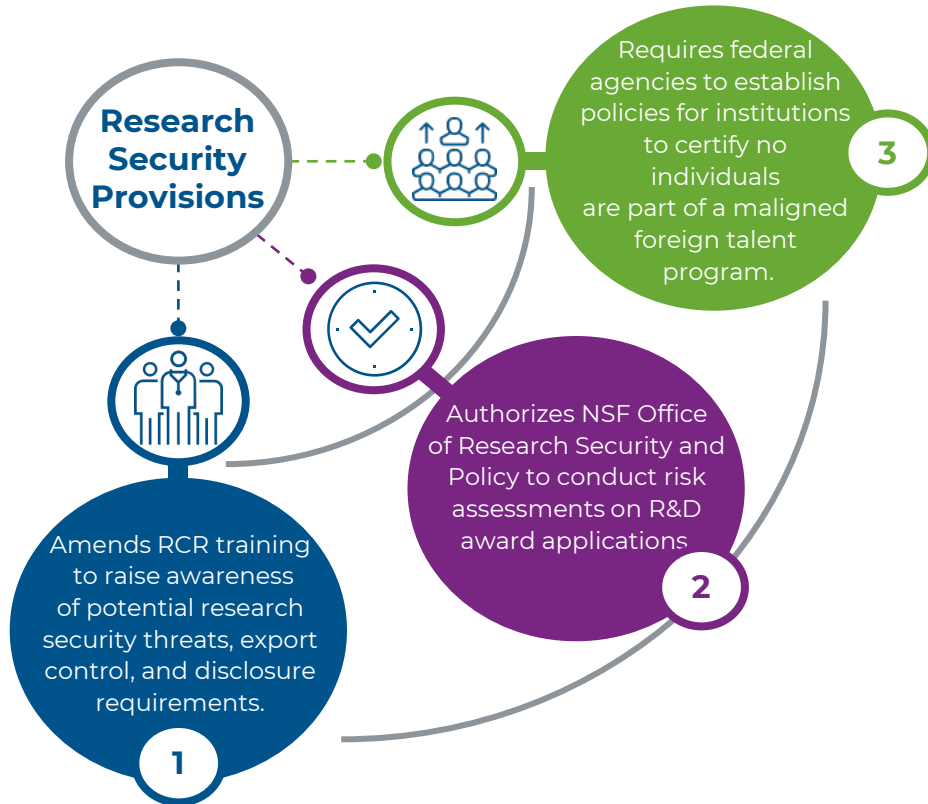
2. Distinguishing intent to deceive from mere failure to disclose/report.

3. Identification of malign actors.

4. Eliminating conflicts of commitment impacting researchers' ability to satisfy funding obligations.

5. Obtaining a thorough accounting of conflicts of interest and retrospective reviews in cases of interest.

Policy Updates: CHIPS and Science Act



- Provides funding for translational semiconductor manufacturing research (which are likely to be restricted in some way).
- Defines foreign countries and entities of concern, as well as foreign talent recruitment programs.
- Expands RCR requirement to all personnel funded by NSF.

**August
2022**

New disclosure types

- On Facilities, Equipment, and Other Resources, disclose support related to proposed project:
 - Visiting scholars & students funded by other entities,
 - In-kind support.
- On Current and Pending (Other) Support, disclose support not directly related to proposed project:
 - Visiting scholars & students funded by other entities,
 - In-kind support with an associated time commitment,
 - Current or pending applications to programs sponsored by foreign governments,
 - Start-up packages from non-proposing organization,
 - Start-up companies based on non-proposing organization intellectual property (IP),
 - **Venture capital added as a disclosure type.**



NSF 2023 PAPPG changes

Other new requirements

- Must use SciENcv for Biographical Sketch and Current and Pending Support documents.
 - Individual must certify these documents are accurate, current, and complete.
- Program officers must request updated Current and Pending Support prior to making a funding recommendation.
- Updated Current support must be submitted throughout the project.
- Authorized Organizational Representatives (AORs) must notify NSF within 30 days of identification of undisclosed Current Support or In-kind Contributions.

Policy Update: RSP Requirements Released

On March 7, 2023, the Office of Science and Technology Policy (OSTP) released a request for information for research security programs required by NSPM-33.



Policy Update: RSP Requirement Timeline



How much flexibility is there?

- Fundamental v. restricted research
- Institution size and research type

How feasible are these standards?

- Implementation of cybersecurity requirements
- Meaningful review and advanced approval of foreign travel
- Availability of documentation of RSP within 30 days of request

Definitions

- “Foreign Government-Sponsored Talent Recruitment Program”
- “Organizational/official business”

Satisfying training requirements

- When are the government funded training modules going to be available?
- Will agencies consistently determine who needs to be trained? At what point in the award process will you know?

NSPM-33 Focus Areas

Actions universities can take now!

Review conflict of interest (COI) and conflict of commitment (COC) programs to ensure the content of disclosures are aligned with the anticipated requirements for federal sponsors.

Ensure business processes across the award life cycle

- from proposal submission, to award receipt and acceptance, to mandatory reporting and monitoring
- can facilitate the review and submission of the requisite disclosure elements, including collecting contracts and digitally signing and attesting to disclosures as required.

Develop new or enhance existing faculty and local research administrator training on required disclosure information in federal funding proposals.



Polling Question #3

Who is primarily responsible for research security at your institution?

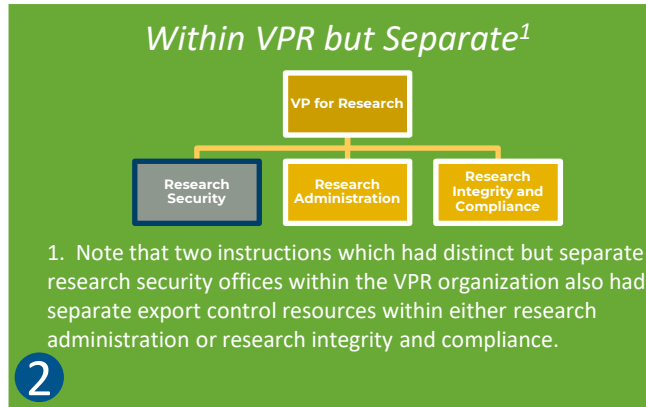
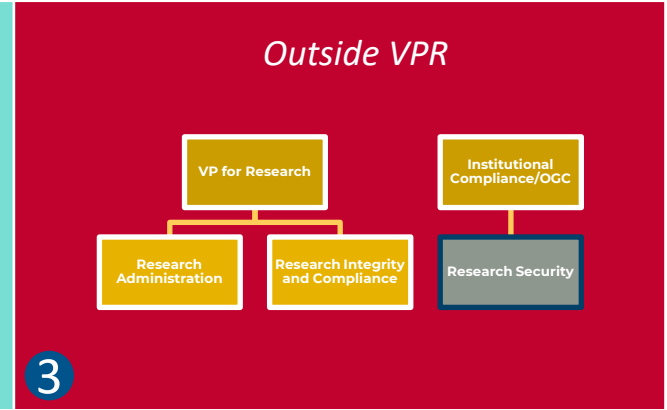
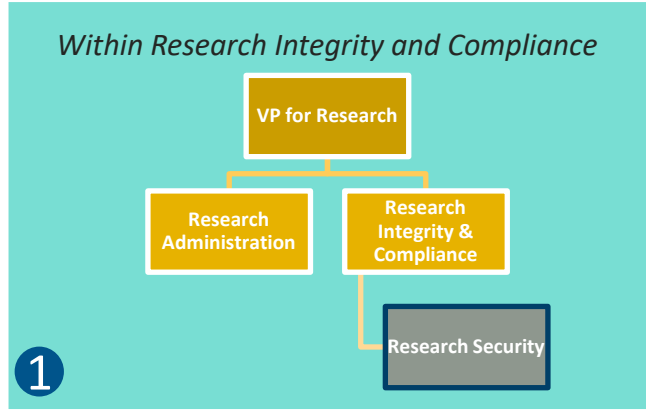
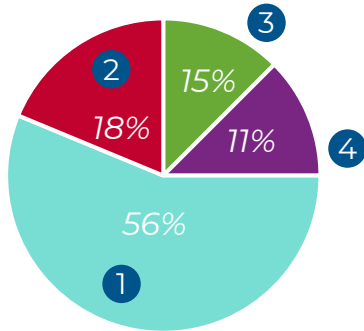
1. Research Integrity and Compliance.
2. Research Compliance.
3. Own Distinct Unit (Within Research).
4. Own Distinct Unit (Outside Research).
5. Not Sure (TBD or Unknown).

Best Practices: Organizational Models

Institutional Benchmarking

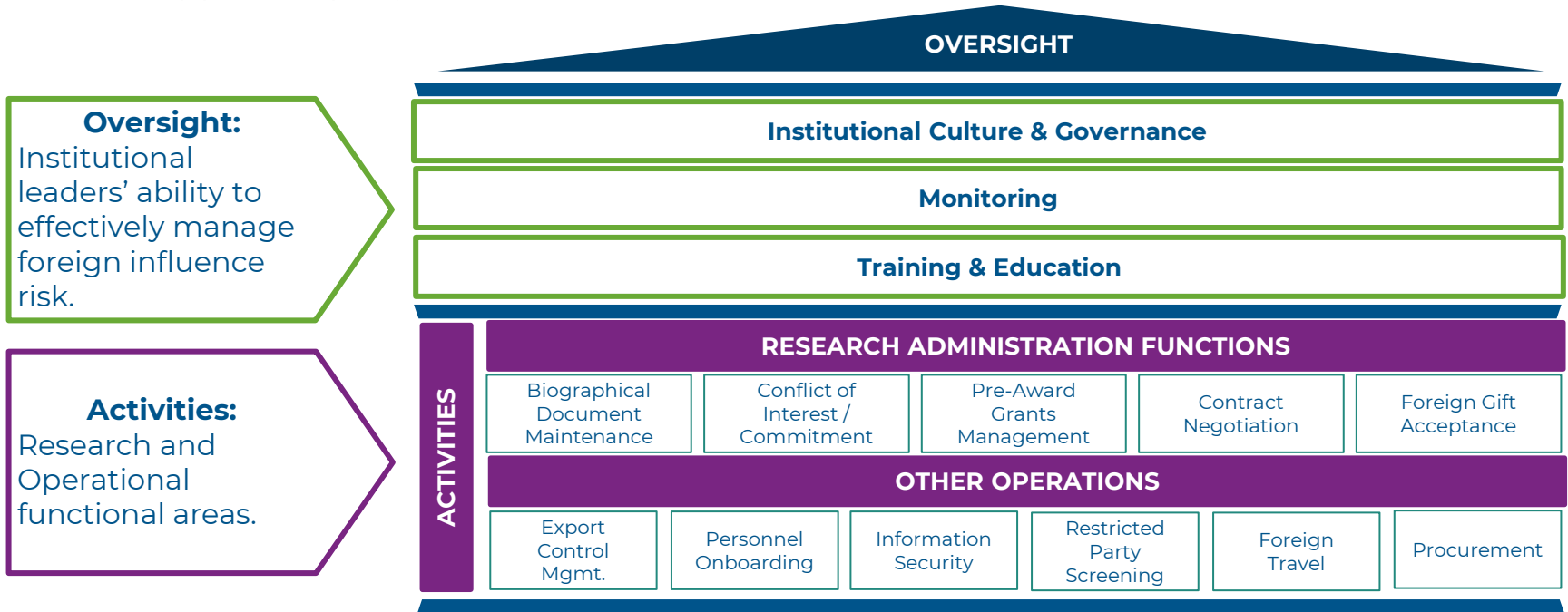
Huron recently conducted an informal benchmarking exercise of 16 RI universities:

- **Only 25% of the cohort had distinct research security teams.**
- Export control functions (which have broader research security duties) revealed emerging trends.



Best Practices: Program Assessment & Development


How do we approach program assessments?



4

ORCID iD's





Connecting research and researchers

[SIGN IN/REGISTER](#)
English ▾

🔍

[ABOUT](#)
[FOR RESEARCHERS](#)
[MEMBERSHIP](#)
[DOCUMENTATION](#)
[RESOURCES](#)
[NEWS & EVENTS](#)

iD

Distinguish yourself in three easy steps

ORCID provides a persistent digital identifier (an ORCID iD) that you own and control, and that distinguishes you from every other researcher. You can connect your iD with your professional information — affiliations, grants, publications, peer review, and more. You can use your iD to share your information with other systems, ensuring you get recognition for all your contributions, saving you time and hassle, and reducing the risk of errors.

FIND OUT MORE ABOUT OUR MISSION AND VALUES

1

REGISTER

2

USE YOUR ORCID ID

3

SHARE YOUR ORCID ID

🔗 Help

Create your ORCID iD

This is step 1 of 3

Per ORCID's [terms of use](#), you may only register for an ORCID iD for yourself. Already have an ORCID iD? [Sign In](#)

First name ?

Last name (Optional)

Primary email

Confirm primary email

Additional email (Optional) ?

+ Add another email

GO BACK

NEXT

Could this be you?

We found some accounts with your name, which means you may have already created an ORCID iD using a different email address. Before creating an account, please confirm that none of these records belong to you. Not sure if any of these are you? [Contact us](#).

First Name	Last Name	Affiliations	View Record
Rebecca	Scott	Birkbeck University of London, University of Reading	View Record
Rebecca	Scott	GEOMAR Helmholtz-Zentrum für Ozeanforschung Kiel, Swansea University, University of East Anglia, University of Exeter	View Record
Rebecca	Scott	American Society for Legal History, Princeton University, University of Michigan	View Record
Rebecca	Scott	Cardiff University, University of Arizona, University of Bath,	View Record

I ALREADY HAVE AN ID, GO BACK TO SIGN IN

NONE OF THESE ARE ME, CONTINUE WITH REGISTRATION

1 2 3

Personal data Security and notifications Visibility and terms

Create your ORCID iD

This is step 2 of 3

Password

.....

- ✓ 8 or more characters
- ✓ 1 letter or symbol
- ✓ 1 number

Confirm password

.....

Notification settings

ORCID sends email notifications about items related to your account, security, and privacy, including requests from ORCID member organizations for permission to update your record, and changes made to your record by those organizations.

You can also choose to receive emails from us about new features and tips for making the most of your ORCID record.

- ✓ Please send me quarterly emails about new ORCID features and tips. *To receive these emails, you will also need to verify your primary email address.*

After you've registered, you can change your notification settings at any time in the account settings section of your ORCID record.

GO BACK NEXT

1 2 3

Personal data Security and notifications Visibility and terms

Create your ORCID iD

This is step 3 of 3

Visibility settings

Your ORCID iD connects with your ORCID record that can contain links to your research activities, affiliations, awards, other versions of your name, and more. You control this content and who can see it.

By default, what visibility should be given to new items added to your ORCID Record?

- Everyone** (87% of users choose this)
- Trusted Organizations** (5% of users choose this)
- Only me** (8% of users choose this)

[More information on visibility settings](#)

Terms of Use

- ✓ I consent to the [privacy policy](#) and [terms of use](#) and agree to my data being publicly accessible where marked as "Visible to Everyone".
- ✓ I consent to my data being processed in the United States.

[More information on how ORCID process your data.](#)

✓ I'm not a robot

reCAPTCHA
Privacy - Terms

Rebecca Scott (0009-0003-8195-1616)

orcid.org/my-record/orcid-0009-0003-8195-1616

Rebecca Scott

ORCID

Connecting research and researchers

https://orcid.org/
0009-0003-8195-1616
[View my public record](#)

Thank you for registering with ORCID
We have sent verification messages to each of your registered email addresses. You will need to verify your primary email address before you can begin adding information manually to your ORCID record.
[Resend verification email](#)

Names

Name
Rebecca Scott

Biography

Activities

▼ **Employment (0)** [Add](#)

Add details of your current and previous employers.
[Learn more about adding employment information to your ORCID record](#)

▼ **Education and qualifications (0)** [Add](#)

Add details about where you have studied and educational or professional qualifications you have been awarded.
[Learn more about adding education or qualifications to your ORCID record](#)

reCAPTCHA
Privacy - Terms

Welcome to ORCID


Rebecca Scott

iD

Your ORCID iD is:
<https://orcid.org/0009-0003-8195-1616>

Your ORCID record is ready

Thank you for verifying your email. You now have access to the full range of ORCID's editing features.



Where do I start?

- > [Add an affiliation to distinguish yourself](#)
- > [Connect your record to other services and start importing your works](#)

Go to my ORCID record

Questions?

Thank you!