



Research Security Policy Updates

*Presentation for COGR
Sarah Stalker-Lehoux
Deputy Chief of Research Security Strategy and Policy
National Science Foundation
June 6, 2024*

TRUST

Trusted Research Using Safeguards and
Transparency

Our Guiding Principles



Respect the science



Get to "YES"



Focus on mitigation measures

Practicing Thoughtful Vigilance...

TRUST

Avoid curtailing beneficial activities due to risk aversion or overly broad interpretation of policy.

Avoid the targeting of individuals based on nationality or country of origin. Protect core values of fairness and due process throughout.

Maintain open lines of communication with the community. We want to hear from you before situations become a major concern.



NSF Responding to Legislative Requirements

Section 10339 of the CHIPS and Science Act

Identify *research areas* ... that may involve access to “**controlled unclassified or classified information**” and “exercise due diligence in granting access to individuals working on such research who are employees of the Foundation or covered individuals on research and development awards funded by the Foundation.”

FY23 Appropriations Report

Open-source research capabilities at NSF could be used by adversaries against U.S. allies or U.S. interests...therefore directs the NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to compile and maintain a list of all NSF-funded open-source research capabilities that are known or suspected to have an impact on foreign military operations.



How did we develop our process?

**February
2024**

JASON Sensitive Research Study

- Assess national security application of the research at the project level

**March
2024**

JASON Rubric Road Test

- NSF proposals lack information for certain evaluation criteria
- Suggestion to use a decision tree rather than a rubric

**March
2024**

NSF Internal Consultations – RSLG, QSSC Road Test

- Development of QIST keywords to use during pilot phase
- Understanding of resources required for Research Security Review Team

**April
2024**

Interagency Consultations – DARPA, NIST, R&E

- Identify mitigation strategy with the research institution
- Benchmarked process and mitigation strategies



TRUST: "Trusted Research Using Safeguards and Transparency"

Evaluate Three Criteria, with transparent step by step process:

- 1) Appointments and positions w/ U.S. proscribed parties and are not a party to a malign foreign government talent recruitment program (MFTRP)
 - U.S. Bureau of Industry and Security Entity List
 - Annex of Executive Order (EO) 14032 or superseding EOs
 - Sec. 1260H of the National Defense Authorization Act (NDAA) for FY2021 - Sec. 1286 of the NDAA for FY2019, as amended
- 2) Nondisclosures of appointments, activities and sources of financial support (current research security policy)
- 3) Potential foreseeable national security applications of the research

OCRSSP will confirm that senior personnel have no **active appointments and positions with U.S. proscribed parties**, and that they are not a **party to a malign foreign talent recruitment program**

Undisclosed information will be examined from the time NSPM-33 Implementation Plan was released (Jan 2022)



TRUST Process

Appointments and positions w/
U.S. Proscribed Parties and
MFTRPs



OCRSSP conduct analytics



Research Security Review Team
to identify mitigation



OCRSSP and the institution will
work together to mitigate risk

Nondisclosures (Current
Research Security Policy)



OCRSSP conduct analytics



Research Security Review Team
to identify mitigation



OCRSSP and the institution will
work together to mitigate risk

National Security Application of
the Research



OCRSSP Keyword Automated
Review



Research Security Review
Team



External USG consultation
coordinated through ODNI (if
needed)



Understanding the Research Security Review Team

5 – 6 members, including:

- The relevant PO / PD
- QIST Subject Matter Experts (~3)
- OCRSSP Staff (1–2)
- External USG QIST and National Security expert (for pilot phase only)
- ***Decision will be a consensus between members***



Research Security Review Team Questions

Are the national security aspects important enough to override the societal benefits of non-national security applications?

Is the technology sufficient and unique enough for the national security use case in mind?

What are the goals of the project?

Guiding Questions



Do certain mitigation measures on the project confer a meaningful advantage to the United States?

Research Security Review Questions continued...

What happens if we say no?

- If the United States has a **definitive advantage**, mitigation makes the most sense when and so can endure the burden of additional protections without negatively impacting the country's relative position.
- If "**neck and neck**," consider whether imposing the burden of security restrictions on U.S. researchers might slow the pace of U.S. innovation relative to foreign competitors.
- If the United States is **not the leader** in this domain, consider whether the United States seeks to benefit from this international cooperation by elevating U.S. capabilities, despite the potential level of risk.



Mitigation Strategies – Examples from DARPA

- NSF is considering some of DARPA's potential risk mitigation strategies that have proven effective when preparing risk mitigation strategies for Countering Foreign Influence Policy issues.
- NSF intends to work with the Federal Demonstration Partnership on sharing mitigation strategy templates
 - 1) Periodic Security Communication
 - 2) Expanded Reporting Requirements
 - 3) Certification of Status
 - 4) Confirmation of Disassociation
 - 5) Proactive Security Measures at Institutions



Example mitigation plan excerpt from DARPA:

- A researcher was rated as a VERY HIGH risk due to multiple active affiliations with PRC government-connected entities (Factor 4 of the DARPA risk rubric) and several instances of active funding from the same entities.
- The Program Manager wanted to mitigate those risks and requested that the institution implement expanded reporting requirements as one part of a multi-faceted mitigation plan.

“The researcher will meet with the institution’s Office of Scientific Integrity on a quarterly basis to review a list of his active collaborations to determine whether there are any changes that should be reported to funding agencies or any additional management/oversight to put in place (e.g., a new COI management plan or modifications to existing plans).”

“On a quarterly basis the institutions will send either an updated list of the researcher’s collaborations or a certified notification that there is no change from the previous submission. These reports will be sent quarterly based on the initial award date of the project.”

“The institution will require the researcher to request permission before engaging in any new foreign collaborations. These collaborations will be vetted by the institution’s Office of Scientific Integrity to determine whether the researcher can begin a collaboration or whether additional mitigation measures need to be implemented.”

“During the six-month reporting period, the researcher will be required to submit an updated SF-424. The SF-424 does have an overall page limitation, which prevented the researcher from including all of his information previously. Going forward, additional pages will be included for any required information that does not fit within the page limit.”



TRUST Implementation

- **Phase 1 – Quantum Proposals – beginning FY25**
 - Pilot program will be an *iterative process* and NSF will assess:
 - Implementation of new Tiger Team process
 - Timeline of process, bandwidth and resources required from NSF staff
 - NSF's ability to assess potential national security application of the research
 - How often NSF needs external consultation
 - ***Continued External Engagement – Listening Sessions with FDP Members, among others***
- **Phase 2 – PAPPG Changes & Expand to some CHIPS+ Key Tech Areas**
 - Information to assess certain criteria are not currently in solicitations
 - Consider expansion to Microelectronics, AI, and Biotechnology.
- **Phase 3 – Scale up Review for all CHIPS+ Key Tech Areas**
 - NSF Staff will have more familiarity with the process
 - Mitigations will be more streamlined, expediting the review process



FFDR
**Foreign Financial Disclosure Reporting -
Requirement**



Sec. 10999b of CHIPS and Science: Foreign financial transactions and gifts

- Requires NSF “recipient institution of higher education... a foundation of the institution, and related entities such as any educational, cultural, or language entity.... to report all “current financial support, the value of which is \$50,000 or more, including gifts and contracts, received directly or indirectly from a foreign source” which is “associated with a foreign country of concern.

Timeline

- First FFDR submission due to NSF by July 31, 2024
- First Year Grace period by September 3, 2024
- Reporting period:
 - July 1, 2023, to June 30, 2024

Tuition payments

- Tuition payments for a specific student(s) are excluded from the reporting requirement. However, if....in the form of a grant, scholarship, or other form of financial aid that stipulates specific criterion...the payment is reportable when the cumulative threshold of \$50,000 from a foreign source is met.

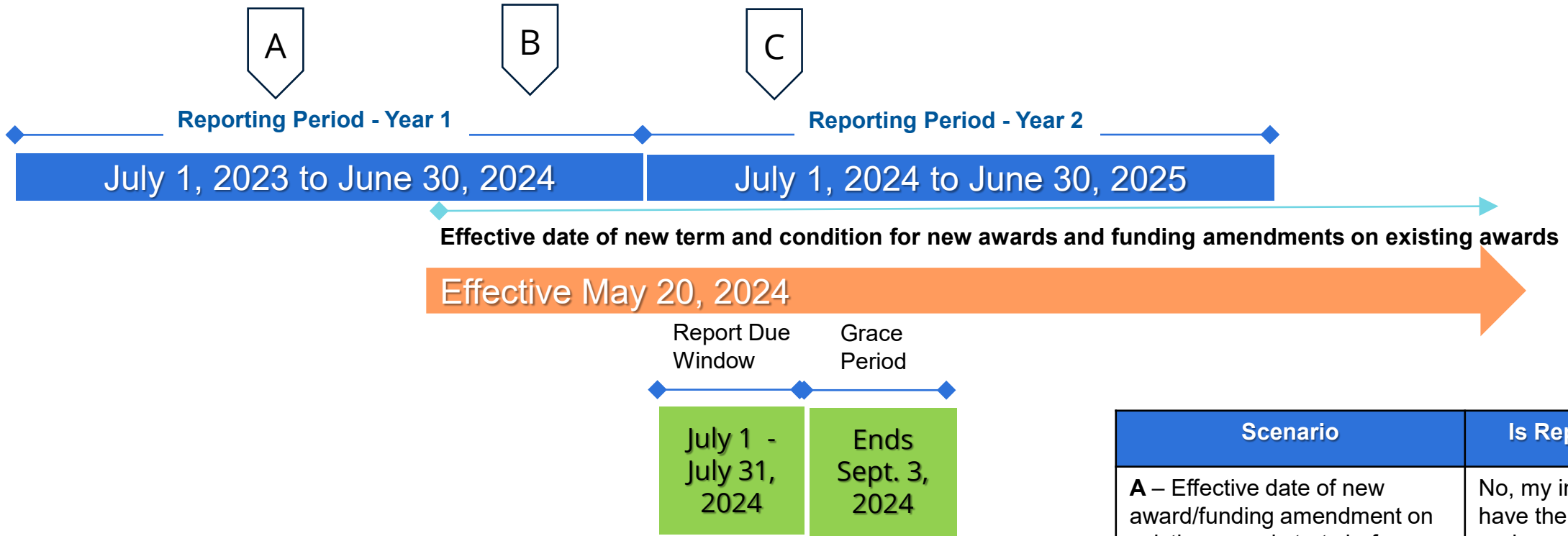


NSF Postaward Foreign Financial Disclosure Report (FFDR) Requirements

- FFDR requirements apply to each IHE that receives an award or funding amendment on an existing award made on or after May 20, 2024
 - Each IHE must submit an institutional report annually – negative reports are required
 - Reporting includes any gift or contract with a cumulative value of \$50K or more per source from a country of concern
 - Reports must be submitted by July 31 each calendar year in Research.gov
 - ***A one-time grace period for submission of the first report has been provided. The grace period expires on September 3, 2024***
 - IHEs must maintain copies of relevant records
 - NSF may request copies of contracts, agreements, or documentation of financial transactions associated with disclosures.
 - Organizations other than IHEs are not required to submit annual FFDR reports
 - A new term and condition has been added implementing this requirement post-award



FFDR Timing



Scenario	Is Reporting Required?
A – Effective date of new award/funding amendment on existing award starts before May 20, 2024	No, my institution does not have the new reporting term and condition and is not required to report
B - Effective date of new award/funding amendment on existing award starts on or after May 20, 2024, but on or before June 30, 2024	Yes, my institution has the new reporting term and condition and is required to report
C – Effective date of new award/funding amendment on existing award starts after June 30, 2024	Report not required in 2024, but my institution will be required to report in 2025



FFDR Portal Key Takeaways

- All FFDR Preparers in the same IHE can create a report in Research.gov, edit an existing report, or submit a report created by another FFDR preparer
- Only one FFDR can be submitted in Research.gov per IHE
- On July 1, 2024, all FFDR Preparers affiliated with an IHE that has received a new award or a funding amendment on an existing award between May 20, 2024, and June 30, 2024, will receive a system-generated email notifying them that the IHE must submit an FFDR for Year 1
- Every IHE organization must submit a negative or positive report in Research.gov
- Foreign support received between July 1, 2023, and June 30, 2024, will report in Year 1 submission window which begins on July 1, 2024
- Once a report is submitted to NSF in Research.gov, it cannot be deleted or withdrawn
- Submitted report for Year 1 can be edited until September 3, 2024. After September 3, the FFDR Preparer must submit a request to Office of the Chief of Research Security Strategy and Policy Office to amend the submitted report
- FFDR is specific to financial support received from a foreign country of concern (i.e., People's Republic of China, Democratic People's Republic of Korea, Russian Federation, and Islamic Republic of Iran)
- If the cumulative value of all gifts and contracts received from a foreign source does not equal or exceed \$50,000, then it is not required to report them in Research.gov



FFDR Future Plans

- Monitor feedback from the research community
- Add “copy” feature to reduce administrative burden for Year 2 and subsequent year reports
- Consider adding capability to download submitted reports
- Enhance post-submission processes (i.e., amendment and extension requests)
- Enhance FFDR functionality based on future PAPPG requirements

 Poll Everywhere [Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) *Ask a question from your seat!*



FFDR Training Resources

- FFDR Demo Site in Research.gov
 - May 20 – June 28, 2024
 - Must have FFDR Preparer role to access demo site in Research.gov
 - All FFDR functionality accessible except report submission and system-generated emails will be disabled
 - Demo data will be deleted prior to opening of reporting period on July 1, 2024
- Research.gov About Foreign Financial Disclosure page Frequently Asked Questions (FAQs)
 - How to Prepare and Submit a Foreign Financial Disclosure Report (FFDR) Guide

 Poll Everywhere [Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) *Ask a question from your seat!*



Save the Date:

Upcoming FFDR Outreach Opportunities

- FFDR Webinar & Demo
 - July 9th at 2:00 – 3:00 PM ET
- FFDR Virtual Office Hours
 - July 16th at 2:00 – 3:00 PM ET
 - July 31st at 2:00 – 3:00 PM ET

 Poll Everywhere [Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) *Ask a question from your seat!*





Contact Information:

Sarah Stalker-Lehoux, Deputy Chief of Research Security Strategy and Policy:
ssalker@nsf.gov

Office of the Chief of Research Security Strategy and Policy Email:
research-protection@nsf.gov

NSF Research Security Website: <https://new.nsf.gov/research-security>



JSR-23-12: Safeguarding the Research Enterprise

Endorsed 2019 themes plus:

- Fundamental research is a critical component of U.S. scientific and technical leadership, ***promoting national security*** in both defense and economic domains.
- Recipients of federal funding have a responsibility to protect U.S. interests, and the ***U.S. research community should be actively engaged in protecting those interests.***
- Transfers of sensitive technologies to foreign countries can create national security risks.
- Research controls, such as CUI, are only one component of a broader strategy of risk mitigation and management to ensure that U.S. research contributes significantly and positively to the national interest.



[Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) ***Ask a question from your seat!***



JASON Key Findings

1. **Openness and transparency** in fundamental research promote scientific discovery, which **improves national security**.
2. International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the PRC to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, **may severely limit the benefits of collaborations with research organizations in the PRC**.
3. Differentiation between sensitive and non-sensitive research is most natural at the **project level**, not at the sub-field level. **Projects in the same sub-field can have very different levels of risk**.



[Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) Ask a question from your seat!



JASON Key Findings (2)

4. Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. **Resources should be concentrated on areas of maximum risk** to ensure that benefits outweigh the costs.
5. Formal controls on research, such as a CUI designation, will have **unintended consequences**.
6. The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects.
7. **Research institutions and NSF have key roles** to play in the process of risk identification and management.
8. Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level.



Poll Everywhere

[Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) Ask a question from your seat!



JASON Key Recommendations

1. NSF should adopt a ***dynamic approach for identifying potentially sensitive research topics*** as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas.
2. NSF should ***proceed with caution before adding access or dissemination controls*** to grants or contracts.
3. The identification of sensitive projects proposed to NSF occurs most naturally ***before peer or panel review***.
4. Specific ***mitigation strategies for sensitive research projects should be negotiated and agreed upon by the PI, NSF, and the institution***.



[Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) ***Ask a question from your seat!***



JASON Key Recommendations (2)

5. NSF should foster a culture of research security awareness by providing ***substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions.***
6. NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

 Poll Everywhere [Pollev.com/cogrstaff949](https://pollev.com/cogrstaff949) ***Ask a question from your seat!***



SECURE

Safeguarding the Entire Community in
the U.S. Research Ecosystem



SECURE Center Timeline

