JASON Report: Safeguarding the Research Enterprise & Updates on Risk Mitigation Approaches at NSF

June 7, 2024

COGR

www.cogr.edu

www.linkedin.com/company/cogr

U

Safeguarding the Research Enterprise

JSR-23-12 Summer 2023

Scott Kemp (study co-lead)
Tom Prince (study lead)
Kate Scholberg (study co-lead)
Rachel Segalman
on behalf of JASON members

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

What is JASON?

- **Independent group of mostly academic scientists and engineers across range of disciplines**
- **Very long appointments – retained history of problems and solutions**
- **Government funded projects across a variety of agencies and subjects**
- **In recent years, several studies for NSF on the topic of research security**

U

Thank you!

To NSF contacts and briefers,
and to JPO staff for making everything run smoothly

Poll Everywhere Pollev.com/cogrstaff949 *Ask a question from your seat!*

U

Outline

- Background and context
- What's changed?
- Some definitions
- Identification of sensitive research
- Risk mitigation strategies for NSF
- An NSF approach to research security
- Proactive steps

U

Outline

- **Background and context**
- What's changed?
- Some definitions
- Identification of sensitive research
- Risk mitigation strategies for NSF
- An NSF approach to research security
- Proactive steps

U

Charge from NSF to JASON

1. What are the general principles that NSF might use in developing lists of research/technology areas of concern?
2. What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?
3. What processes might NSF establish for annually reviewing its list of research/technology areas of concern?
4. Using one or more specific research/technology areas, as examples, what detailed evaluation criteria might NSF use for identifying research/technology areas of concern?
5. What are some of the potential impacts on the research community should some NSF-funded research areas be designated as areas of concern?
6. What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?

U

We have been here before

- How to ensure US research security without undermining benefits of S&T
- 1980s: Soviet technology acquisition
  - Corson report (1982): “Scientific advance requires world wide access to all prior findings…”
  - 3 categories of research:
    - Activities where openness is a massive asset
    - Activities which should be classified
    - “Grey” area
- What’s different? Increasing perception that national security is related to advances in civilian commercial sector
  - Constellations of satellites, AI & Large Language Models

U

What's different?

- Increasing perception that national security is related to advances in civilian commercial sector
  - Constellations of satellites, AI & Large Language Models
- Decreasing distance between academic research and applications (NSF TIPS Directorate)
- Globalization of research enterprise
- Rise of PRC as a peer competitor
- Regulations and Legislation

U

2019 JASON report

JSR-19-2I

Fundamental Research Security

Concerns must be taken seriously, but openness is often of net benefit to national security.

We reaffirm the findings and recommendations of this study, which are still entirely relevant.

JASON 2019 Finding: **National Security Decision Directive (NSDD) 189**, established in 1985 a clear distinction between fundamental research and classified research. This **remains a cornerstone to the fundamental-research enterprise**, as officially reaffirmed in 2001 and 2010 and it continues to inform policy today.

U

2019 JASON report

Specific findings and recommendations of the 2019 report regarding CUI:

JASON 2019 Finding: Universities have mechanisms to handle Controlled Unclassified Information (CUI) under existing categories, such as HIPAA, FERPA, Export control, and Title XIII. CUI protection is difficult, but suited to these tasks, however it is **ill-suited to the protection of fundamental research areas**.

JASON 2019 Recommendation: NSF should support reaffirmation of the principles of NSDD-189, which make clear that fundamental research should remain unrestricted to the fullest extent possible, and should **discourage the use of new CUI definitions as a mechanism to erect intermediate-level boundaries around fundamental research areas.**

In this study, given new context, we revisit these

U

Value of Academic Research to National Security

2023 findings abstracted from prior JASON report

Finding: **Fundamental research has historically contributed to U.S. security** and it continues to do so.

Finding: **Openness and transparency** in fundamental research promote scientific discovery, which **improves national security**

U

Outline

- Background and context
- **What's changed?**
- Some definitions
- Identification of sensitive research
- Risk mitigation strategies for NSF
- An NSF approach to research security
- Proactive steps

U

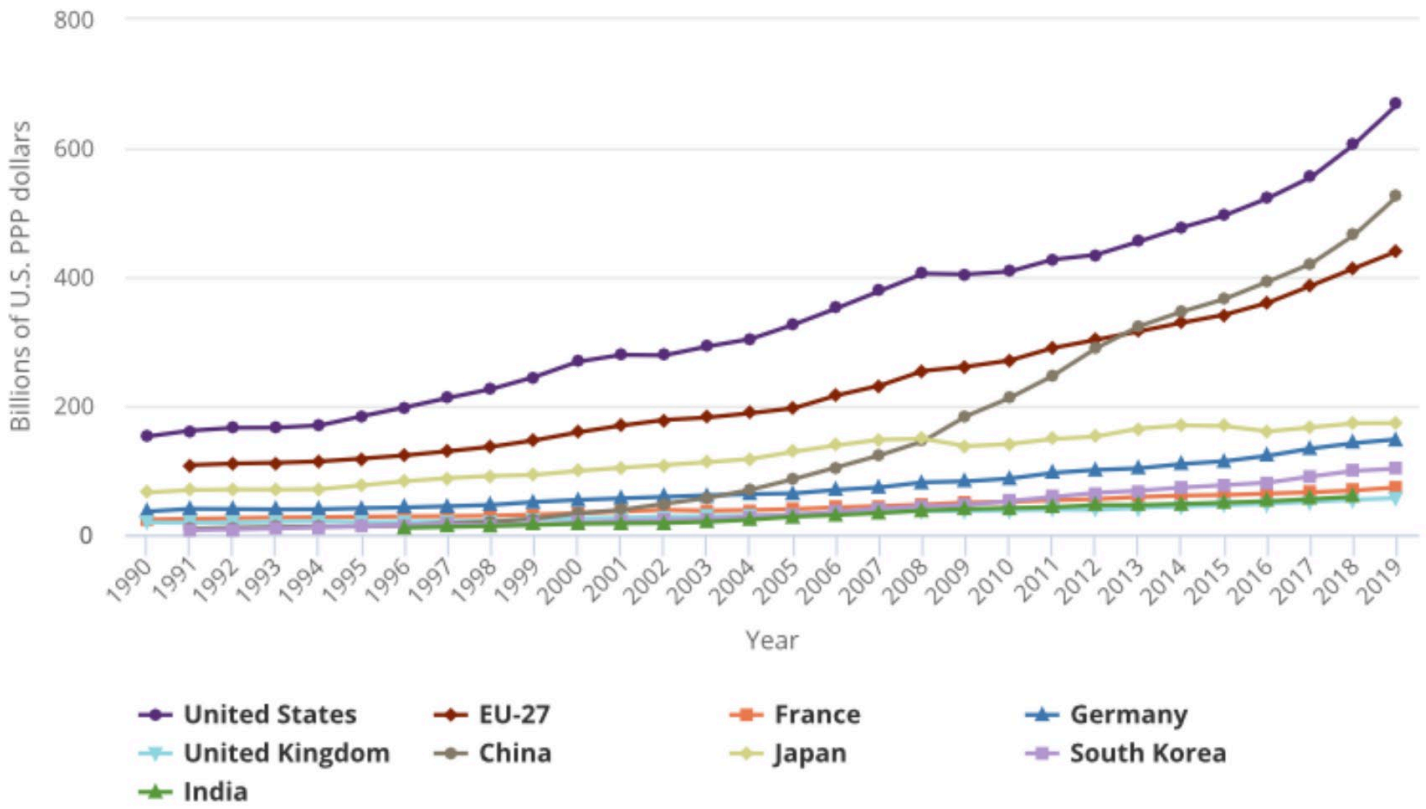
Recent Legislation

- In June 2022, the Committee Report to the FY2023 Appropriations Bill encouraged the NSF to
  - Create clear guidelines that inform researchers and universities on disclosure requirements pertaining to research security.
  - Encourages NSF to continue to engage university and affinity groups to listen to any community concerns [about research security].
  - 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**.

- Later, in August 2022, the **CHIPS and Science Act** directed the NSF to:
  1. identify research areas supported by the Foundation... that may involve access to [already designated] **controlled unclassified or classified information**
  2. exercise due diligence in granting access, as appropriate, to the CUI [Controlled Unclassified Information] or classified information identified under paragraph (1)

U

Changing Situation vis-à-vis the PRC



- China has continued to invest in R&D and gain scientific and technical prowess
- PRC funding of higher ed has doubled in last decade → surpassed US in scientific publications
- This is not a problem in itself; more problematic is PRC's widespread acquisition of U.S. technology through duplicitous or illegal means

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Chinese Military-Civil Fusion (MCF)

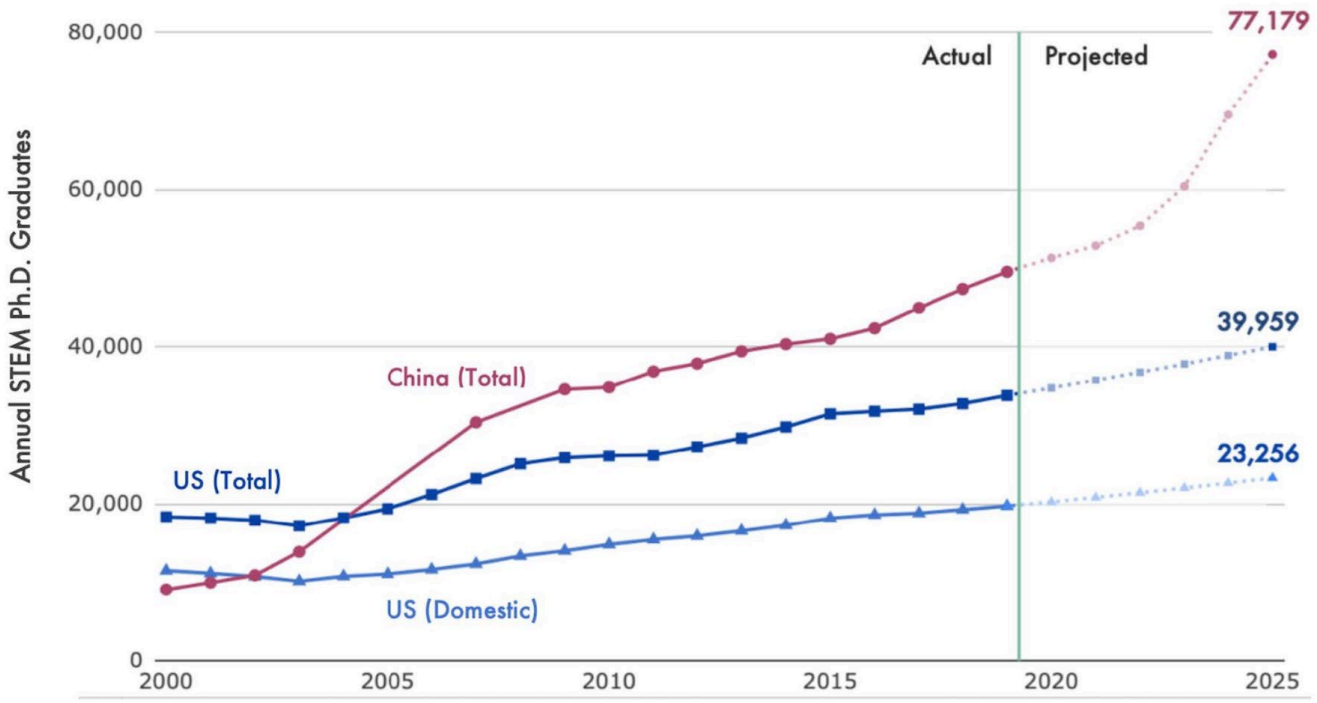
- In the US, there is voluntary cooperation between the government and private sector via R&D funding of grants and contracts
- In contrast PRC's MCF is a state-led program meant to leverage all state, academic, and commercial developments to strengthen the Chinese military. Specifically, it aims to "Establish a complete policy and institutional system for SC (science & technology) military-civil fusion" *
  → leads to restriction of information flow from Chinese universities/institutions

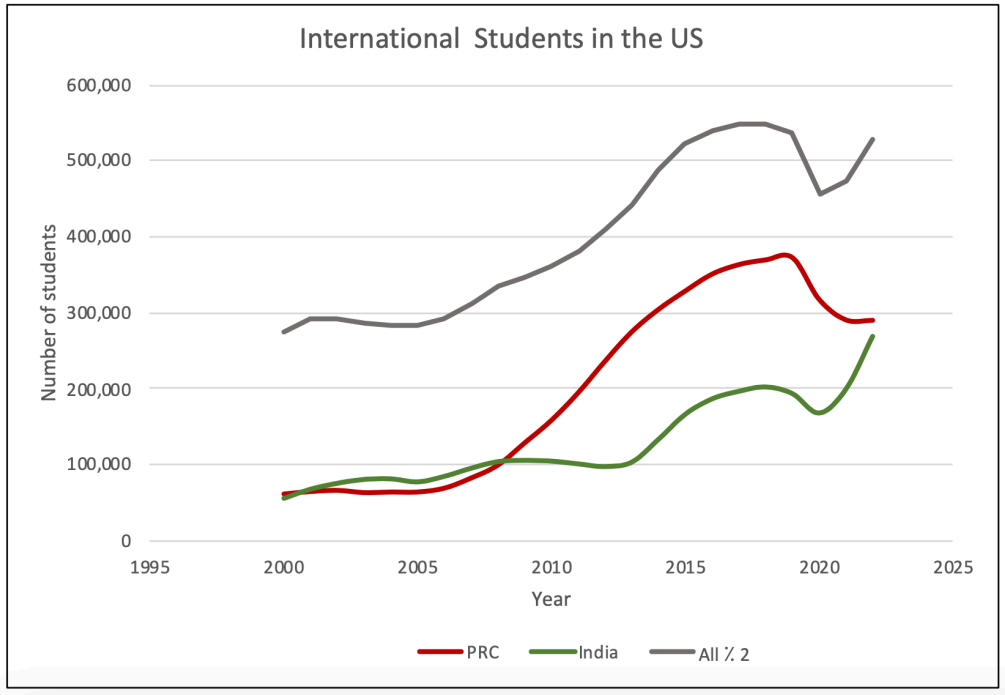
- Finding: international collaborations with those who share the ideals of openness and transparency benefit all participants. However, the PRC's recent effort to preferentially direct fundamental research towards military needs, and the decisions to restrict the flow of information out of the country, may **severely limit the benefits of collaborations with research organizations within the PRC.**

*The "13th Five-Year" Special Plan for ST Military-Civil Fusion Development "", PRC Ministry of Science and Technology (MOST;)

U

STEM graduates in China vs US





- STEM graduates in the PRC have rapidly grown over the past few decades, outpacing the US

- Overall, international students in the US have recovered since the pandemic, but not those from PRC

U

Outline

- Background and context
- What's changed?
- **Some definitions**
- Identification of sensitive research
- Risk mitigation strategies for NSF
- An NSF approach to research security
- Proactive steps

U

Some Definitions [in the context of this study]

National Security: the protection of the United States, its citizens, and its interests at home and abroad from threats [specifically, from misappropriation of R&D]; entangled with economic security, but our focus is national defense.

Research and Development: includes **both basic and applied research**, as well as experimental development

Fundamental research: as defined by NSDD-189, basic and applied research in science and engineering, **the results of which are ordinarily published and shared broadly within the scientific community**. Federally funded development work is not considered part of fundamental research.

Fundamental research exclusion (FRE): FRE provides that research for which no publication, dissemination, or access restrictions have been accepted is **excluded from export control regulations**. The **exclusion is voided if publication approval is required by the sponsor or the government or if citizenship-based restrictions have been accepted.**

U

Some Definitions [in the context of this study]

Sensitive Research

- Could **likely evolve in the future** to have a **direct and predictable impact on national security**
- But the research is **not yet sufficiently advanced to know what level of impact i**t might have in the future.
- Some degree of **risk mitigation** is appropriate, but not necessarily formal controls.
- Would **retain the FRE**

Highly Sensitive Research

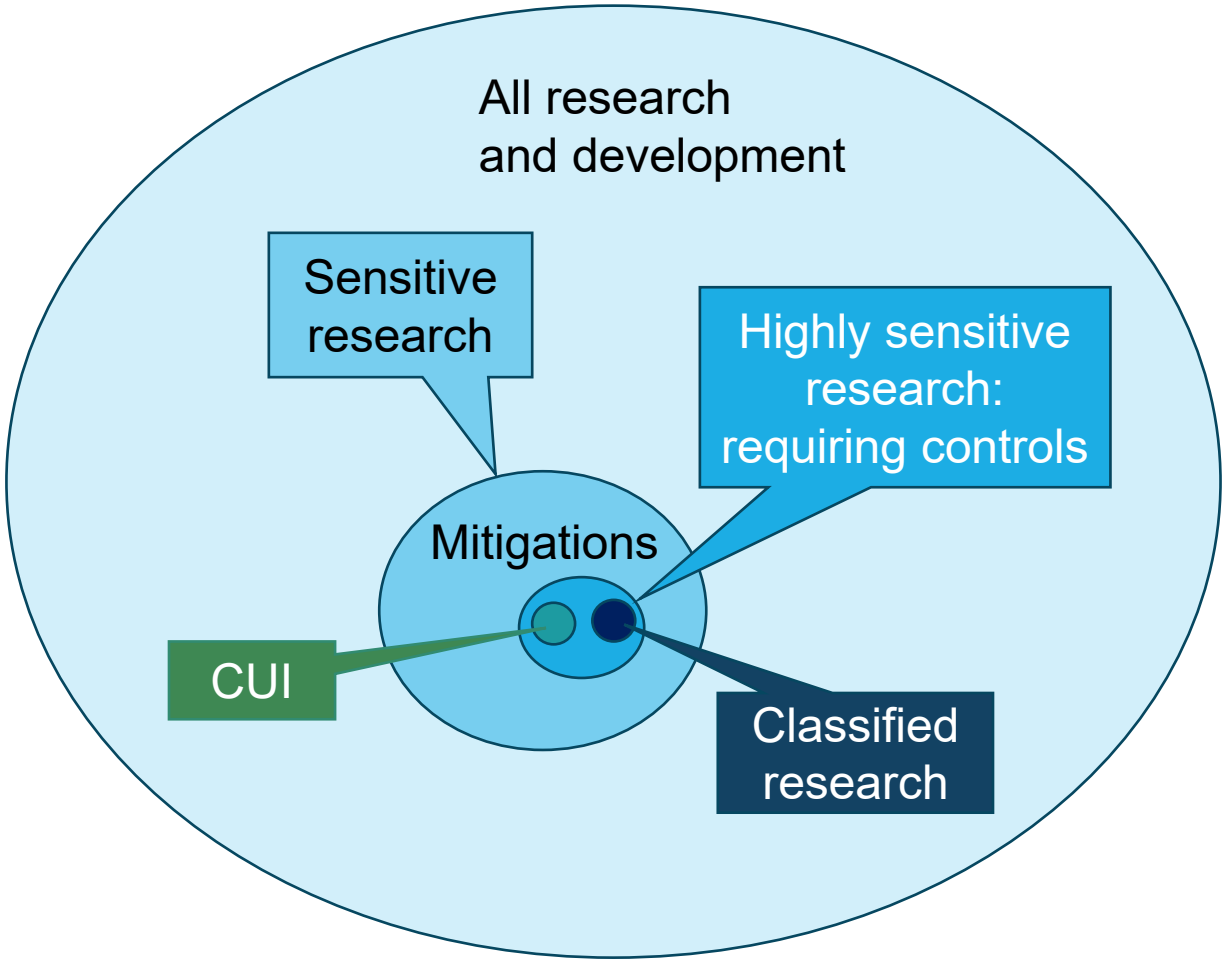
- Has a **demonstrable direct and predictable impact on national security**.
- **Formal controls (restrictions)** are appropriate.
- The **FRE is voided.**

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Relationships Between Definitions

- Mitigations are required for any sensitive research
- Controls are a more extreme form of mitigation– **restrictions for which FRE protection is forfeited**
- CUI is a form of control, but not the only form
- Classification is the most extreme form of control



Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Outline

- Background and context
- What's changed?
- Some definitions
- **Identification of sensitive research**
- Risk mitigation strategies for NSF
- An NSF approach to research security
- Proactive steps

U

Identification of Sensitive Research

How do we decide what research is sensitive?

- By PI or researcher?
- By topical area?
- By collaborative entity?
- Or, by other criteria, such as application readiness?

Approaches have different benefits and drawbacks, depending on context

U

DOD Approach: Researcher-Based Risk Review

Policy for Risk-Based Security Reviews of Fundamental Research that is to be applied to all projects selected for funding

- Recognizes that international collaborations are helpful
- Acknowledges that "know-how" is important
- Mainly focuses on collaborations with Foreign Countries of Concern (China)
- May inadvertently disincentivize some populations

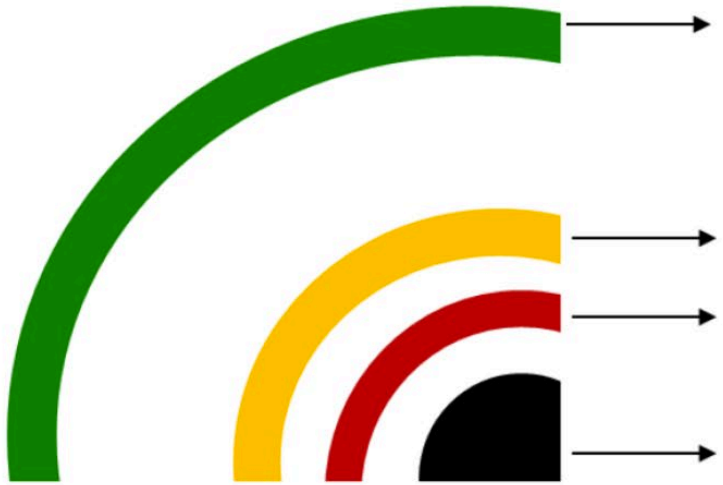
	Factor 1: Foreign Talent Recruitment Programs	Factor 2: Funding Sources	Factor 3: Patents	Factor 4: Entity Lists
Prohibited factors				
Discouraged; mitigations needed or else rejection				
Mitigations recommended				
Mitigations suggested				
No mitigations needed				

specific conditions

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

DOE Approach: Critical Technology Identification



S&T Green Technologies and other non-sensitive DOE R&D: Publication and IP Review/Protection + other standard controls/protections

S&T Yellow Technologies: Publication & IP Review/Protection + may require additional controls/protections and enhanced monitoring

S&T Red Technologies: Publication and IP Review + restrictions on certain transactions with CORs and additional controls/protections

Classified/Export Control Protected Technologies: Applicable Classification and/or Export Control protections

- Based on technologies, with yearly review
- Applies only to national labs
- **Likely requires significant resources to implement**
- Unclear impact on international collaboration

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

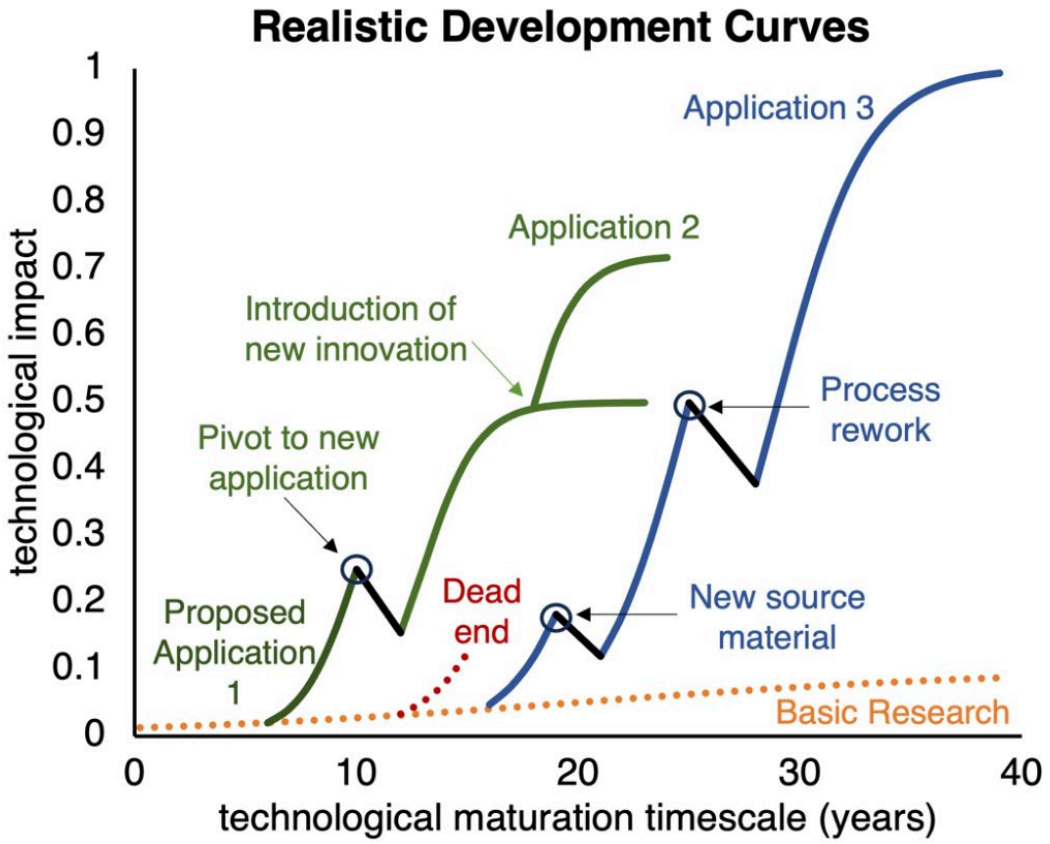
Different Identification Approaches

- DOD and DOE approaches are tuned to be appropriate for those agencies' specific issues and communities
- What other considerations are there for identification of sensitive research?

U

How are Technologies Created?

The development timescale also matters and is very hard to predict



Basic research related to propagation of electromagnetic energy
Electromagnetic bandgap structures in split ring resonators and optical fiber waveguides
Invisibility cloaks
Metastructure-based low-profile antennae

- Sometimes it's just hype
- ... but sometimes things mature rapidly or change direction, or build on each other nonlinearly
- ....and it's hard to know in advance what will happen

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Technology Readiness Levels

Technology Development Stage	TRL	Definition
Fundamental Research	1	Basic principles observed and reported
	2	Technology and/or application concept formulated
Research and Development	3	Experimental proof of concept
	4	Validation of component(s) in a laboratory environment
	5	Validation of semi-integrated component(s) in a simulated environment
Pilot and Demonstration	6	System and/or process prototype demonstrated in a simulated environment
	7	Prototype system ready (form, fit and function) demonstrated in an appropriate operational environment
	8	Actual technology completed and qualified through tests and demonstrations
Early Adoption	9	Actual technology proven through successful deployment in an operational environment
Commercially Available		Technology development is complete

- Only occasionally does low TRL correspond to sensitive research

U

Evaluation of National-Security Significance

- Not all High TRL level work is of National Security Significance
  - What is the international state of readiness?
  - Is there a clear advantage to US protections?
  - National Security Applications?
  - Do other applications (societal good) outweigh national security concerns (seismic monitoring example)
- Can't be done by field or sub-field
- Context/details matter

Evaluation of National-Security Significance

- Scoping of the subfield for consideration is challenging
  - fields organize themselves differently, often for historical reasons

Example: quantum sensors within Quantum Information Science

Consider a clock:

- $\Delta f/f = 10^{-19}$ at concept level, vs
- $\Delta f/f = 10^{-15}$ with a 1-liter volume that has operated in space

→ potentially sensitive
(military applications in satellites)

Not all technologically advanced clocks are sensitive, nor all 1-liter clocks... depends on the context

https://www.nasa.gov/directorates/somd/space-communications-navigation-program/deep-space-atomic-clock-dsac-overview/

Identification of Sensitive Research

Finding: Differentiation between sensitive and non-sensitive research is most natural at the **project level, not at the subfield level**.

Finding: Risk mitigation needs to 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.

- Recommendation: The 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. NSF's process of identifying sensitive research projects should:
- (a) Differentiate research projects based on the **sensitivity of their potential applications**
- (b) **Include the maturity of the development path (Technology Readiness Level - TRL) f**or potential applications in the assessment of risk, and
- (c) Include an assessment of the **direct and predictable national security impact** of the applications of a successful proposal.

U

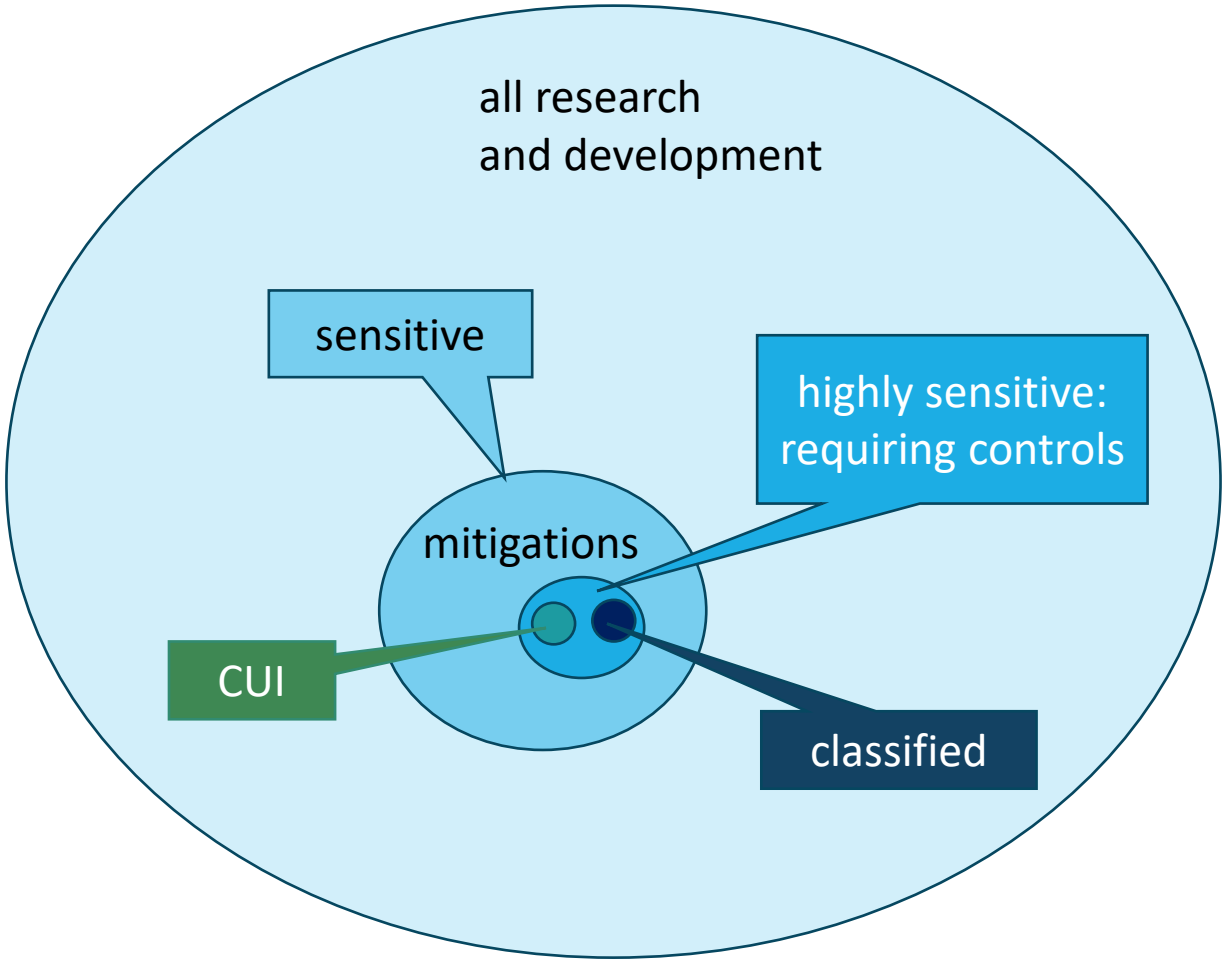
Outline

- Background and context
- What's changed?
- Some definitions
- Identification of sensitive research
- **Risk mitigation strategies for NSF**
- An NSF approach to research security
- Proactive steps

U

Mitigations vs Controls

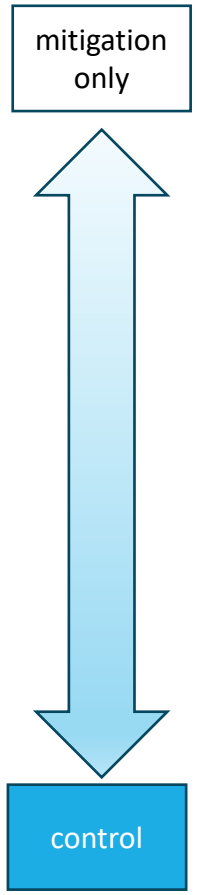
- Mitigations are required for any sensitive research
- Controls are a more extreme form of mitigation– **restrictions for which FRE protection is forfeited**
- CUI is a form of control, but not the only form
- Classification is the most extreme form of control



Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Potential Mitigations and Controls



- Changes to the scope of a research grant
- Training/enhanced training of the PI (risks, publications, personnel)
- Increased frequency or scope of reporting
- Physical security standards for laboratories or computational facilities
- Cyber-security standards for laboratories or computational facilities

Sensitive

- Restrictions on participation for individuals of concern
- Mandatory pre-approval for conferences or publication
- Mandatory pre-approval Open Source data or software
- CUI-like protections
- [Funding contingent on accepting classification]

Highly Sensitive

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

Unintended Consequences of Controls

- Loss of fundamental research exclusion
- Increased cost of research
- Reduction in number of U.S. research organizations engaged in fundamental research important to national defense
- Shrinking of talent pipeline
- Inhibiting competitive development of new technologies
- Possible increased bureaucratic overhead at NSF

costly in $$$

costly in talent and workforce development

costly in idea exchange for national competitiveness

U

Unintended Consequences of Controls

Finding: Formal controls on research, such as CUI, will **have unintended consequences** including: increasing the cost of doing research, diverting resources better applied to increasing the U.S. research effort in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research in critical fields.

Recommendation: **The NSF should proceed with caution before adding access or dissemination controls to grants or contracts**. In considering whether to apply formal controls to a sensitive research project, the NSF should consider the balance between the positive protective benefits and unintended negative consequences of controls. Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and military interests.

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

U

Outline

- Background and context
- What's changed?
- Some definitions
- Identification of sensitive research
- Risk mitigation strategies for NSF
- **An NSF approach to research security**
- Proactive steps

U

A Research Security Approach Tailored for NSF

- A large fraction of NSF-funded research is fundamental
- NSF does not manage laboratories*; mostly university & consortia grants and contracts
- Primarily awards **in response to proposals**
- Extensive international collaboration
- Much of the NSF-funded community may not be aware of research-security concerns

* exception for large scientific facilities, not addressed here

U

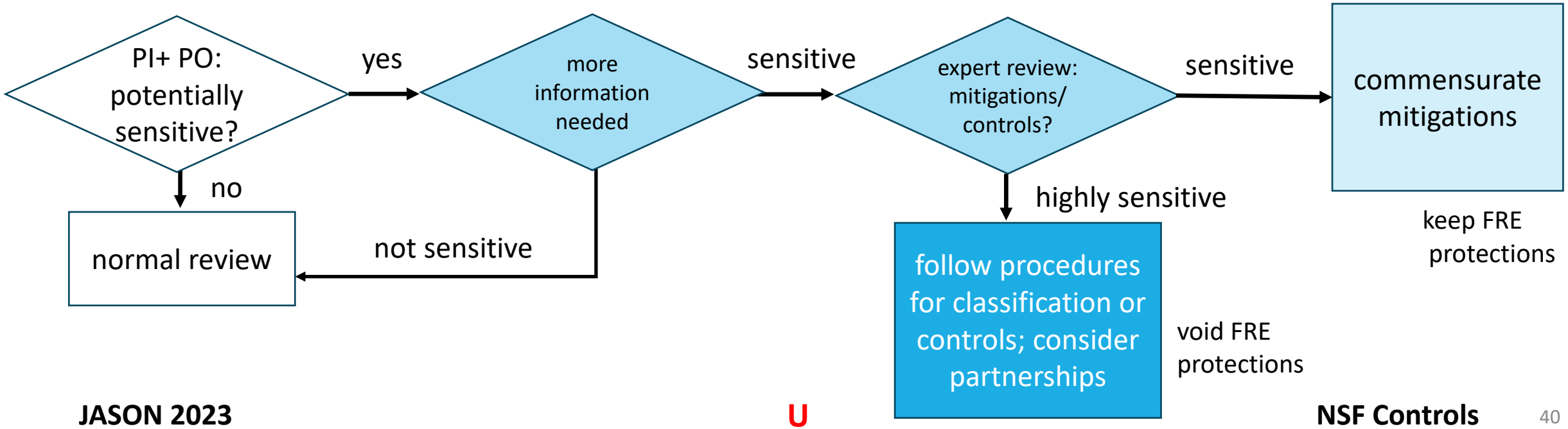
A Project-Driven Approach

Finding: The NSF **proposal review cycle** provides the best and most natural means for identifying sensitive projects

Recommendation: The identification of sensitive projects proposed to the NSF occurs most naturally before the peer or panel review. **We recommend that the PI and the NSF program officer, with guidance from the Division Office, determine if a proposal constitutes a sensitive project.** The NSF may wish to **implement a pilot program** within some division of the NSF to gain experience with the process. The NSF should consult with other federal research funding agencies such as DOE, NIH, and DOD to help identify sensitive research.

Suggested Process

1. For non-sensitive research → normal review process
2. For research deemed sensitive, use additional information and expert advice to determine appropriate mitigations
3. If controls are required, such that NSDD-189 no longer applies:
   - if the project must be classified, follow existing procedures
   - if controls but not classification are needed, consider partnering with another agency



U

Information Needed for Further Review

Further information needed from PI if "yes" answer to national security sensitivity question: [list to be developed; these are draft suggestions]

1. The intended use (if any) of the results of this project.
2. The technology readiness level (TRL) of the work now and expected at the end of the proposal.
3. Whether the technology has features that create national security impact beyond that of technology already discussed in the open literature.

Information can be included in the Broader Impacts section of the proposal to decrease extra burden on PI

U

Deciding on Actions for Sensitive Projects

Recommendation: Specific mitigations on sensitive research projects should be **negotiated and agreed upon by any PI, the NSF, and the sponsored-projects office of the institution** accepting responsibility for the execution of the research. Specific mitigation steps should be proportional to the assessed risk relative to the associated costs.

1.How the intended, or realistically foreseeable, uses of the technology might impact U.S. national security.
2.The relative stage of advancement of the United States versus other countries in this research area.
3.The impact of restrictions on the ability of some researchers to work on this project.
4.The impact of controls on communication of results of the research on the PI's ability to successfully carry out the research and on the community at large.
5.Additional costs, financial and otherwise, of the proposed mitigations or controls.

U

Outline

- Background and context
- What's changed?
- Some definitions
- Identification of sensitive research
- Risk mitigation strategies for NSF
- An NSF approach to research security
- **Proactive steps**

U

The Role of Universities

Finding: Research institutions and the NSF have key roles to play in the process of risk identification and management. Dialogue between the NSF and research institutions such as universities is critical.

Recommendation: The NSF Office of Research Security should initiate meetings and forums with universities to discuss its plans for research security and to solicit input and feedback on its procedures once they begin to be implemented. This can begin now with respect to research-security training modules being developed by the NSF. If the NSF initiates a pilot program for the identification of sensitive or highly sensitive research and its mitigation, feedback from universities will be very important in tuning the program for wider implementation across the entire scope of NSF-funded research.

U

Building a culture of awareness of research security

Take inspiration from successes of "safety culture"

Finding: Awareness of research-security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level and such steps are mandated under the CHIPS and Science Act.

Recommendation: The NSF should foster a culture of research security aware- ness by providing substantive information to researchers about real risks, resources from which researchers may voluntarily seek guidance, and by ongoing engagements with researchers and their institutions about the efficacy of research mitigations and controls

- Designing security procedures in such a way that researchers understand what is being protected and how to implement the procedures effectively.
- Providing researchers with nontrivial information and examples about real risks.
- Providing resources for researchers to ask for research security guidance.
- Providing researchers a place to report concerns ("if you see something, say something"). Researchers will need to understand that their concerns will not result in bias against or profiling of colleagues.

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

U

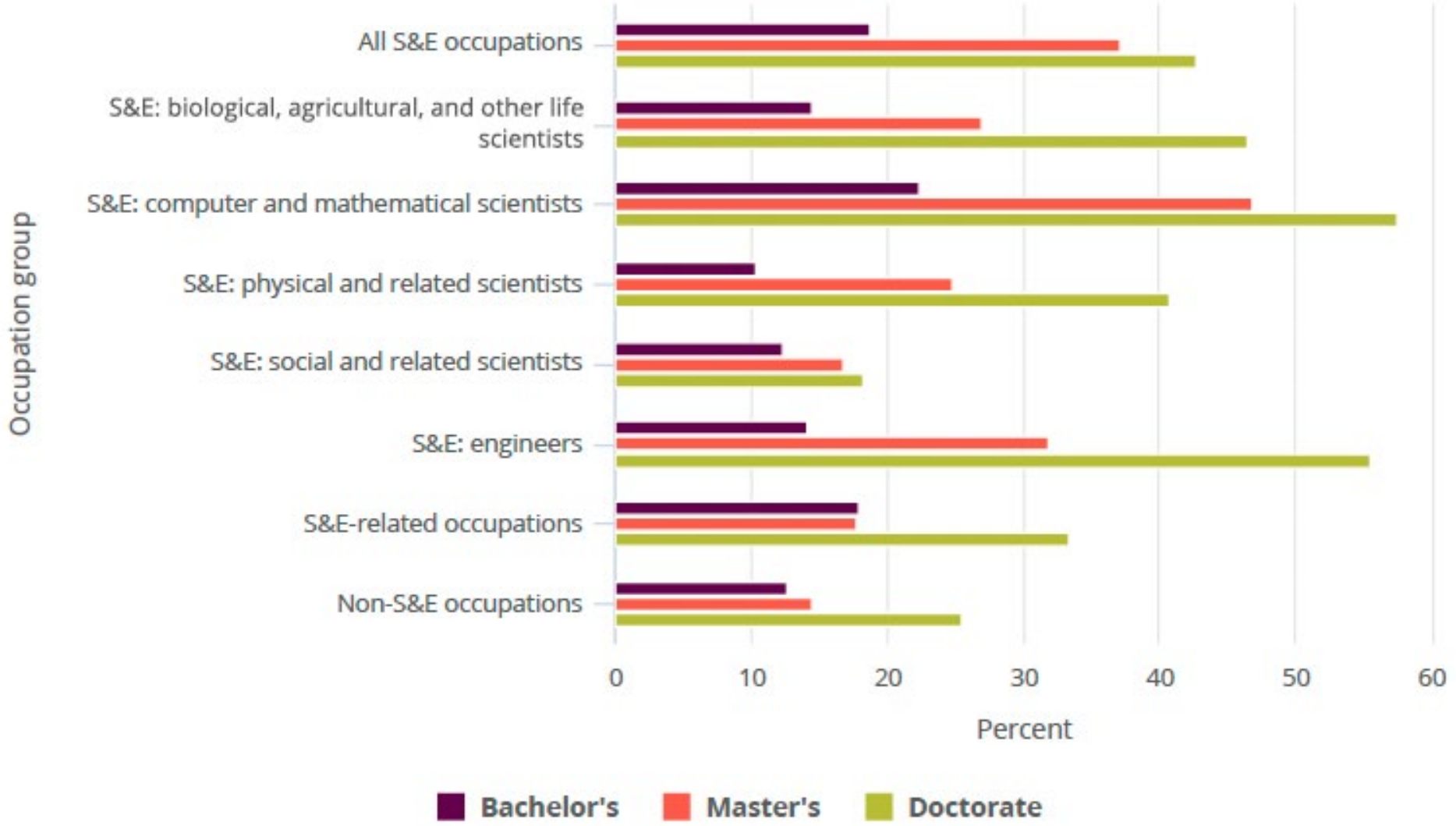
Proactive Steps

- Capitalize on **international relationships with allies**

Recommendation: The 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.

- **Address shortages in the U.S. STEM workforce**
  - 70% of foreign born doctoral students choose to stay in the US after degree → critical part of STEM pipeline
  - US STEM workforce of 36 million needs constant stream of early career trainees → US currently faces a shortfall of ~5,500 students/year
- Increase investment in key technological areas of importance to the country.

Foreign-born share of workers with a bachelor's degree or higher, by highest degree level and occupation group: 2021

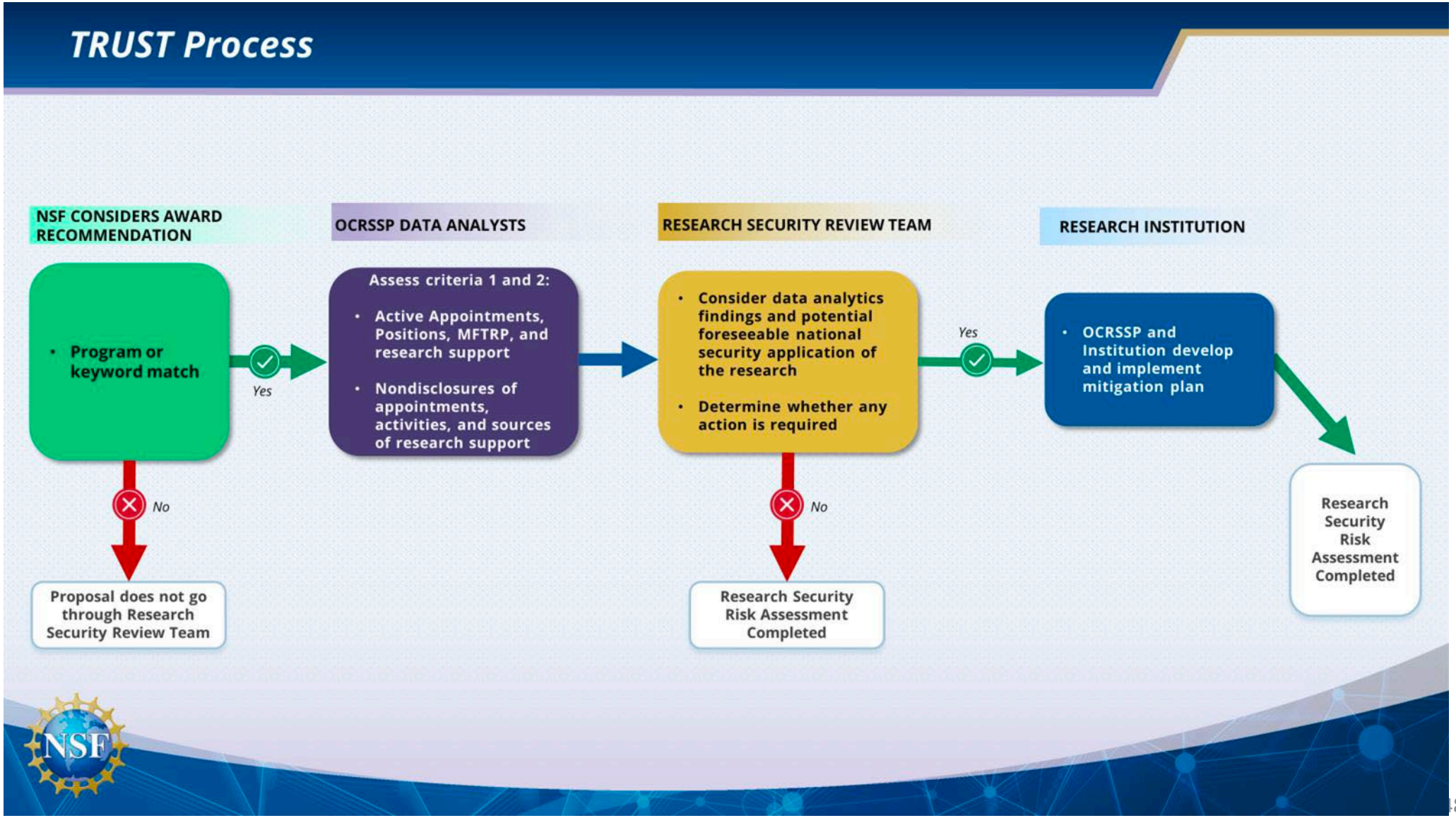


National Center for Science and Engineering Statistics | NSB-2024-3

Source(s):
NCSES, NSCG, 2021.

Indicators 2024: Labor Force

Breaking News: NSF TRUST framework



U

Summary of Key Recommendations

- **Controls should be used with caution** as they remove the fundamental research protection and create hindrances for research
- **Apply FRE-preserving mitigations for sensitive projects** if at all possible or **partner with other agencies** if control needed
- Weigh the unintended **negative consequences against the security benefits**
- Initially identify sensitive projects **at the proposal level**, before review
  - initial assessment by the PI with review by the NSF program officer
  - **TRL level** matters, as does relative stage of advancement wrt other countries
  - Employ **expert advice**
- Start with a **pilot program**
- Take **proactive steps** for US leadership and training of workforce

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***