



Establishing your Research Security Program

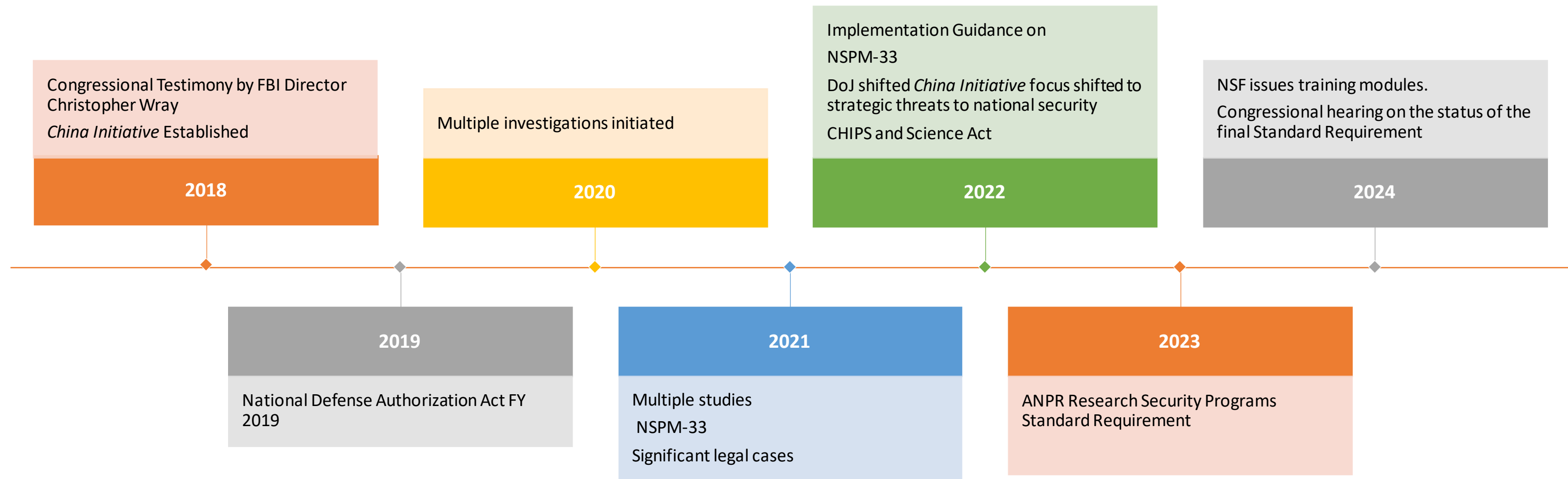
SRAI Virtual Conference | Wednesday, May 8, 2024

Susan Wyatt Sedwick | Sr. Consulting Specialist | | SRAI Distinguished Faculty

Learning Objectives

1. Understand good practices in research security.
2. Respond to allegations or suspected non-compliance.

Chronology





Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022.

- 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

Source: Report on Research Compliance. September 21, 2022. *NSF, OSTP Begin Implementing CHIPS Act.* V. 19, No. 10.

Current Countries of Concern

- China (along with Hong Kong and Macau)
- Russia
- Iran
- North Korea
- Cuba
- Venezuela



Federal Register Notice 88 FR 14187

PUBLISHED DOCUMENT

AGENCY:

Office of Science and Technology Policy (OSTP).

ACTION:

Notice and request for comments.

SUMMARY:

The Office of Science and Technology Policy (OSTP) requests comments from the public on draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). The draft Standard Requirement has been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementing this requirement.

DATES:

Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023.

DOCUMENT DETAILS

Printed version:

[PDF](#)

Publication Date:

[03/07/2023](#)

Agency:

[Office of Science and Technology
Policy](#)

Dates:

Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023.

Comments Close:

06/05/2023

Document Type:

Notice

Document Citation:

88 FR 14187

Page:

14187-14189 (3 pages)

Document Number:

2023-04660

Research Security Training

 [View image credit](#)

Upcoming service outages Scheduled service outages will take place every Thursday evening. During this time, the research security training modules may be temporarily unavailable.

[Home](#) / [Research Security](#) / **Research Security Training**

The U.S. National Science Foundation, in partnership with the National Institutes of Health, the Department of Energy and the Department of Defense, is sharing online research security training for the research community.

This training provides recipients of federal research funding with information on risks and threats to the global research ecosystem — and the knowledge and tools necessary to protect against these risks.

<https://new.nsf.gov/research-security/training>

On this page

- [Take the research security training](#)
- [Deploy your own instance of the training](#)
- [Frequently asked questions](#)
- [Contact us](#)

Feedback

Proposed Research Security Programs Standard Requirement

- Covered Research Organizations
- Effective one (1) year from issuance of the final memorandum
- Annual institutional self-certification of compliance through SAM.gov
- Description of program on a publicly-accessible website
- Definitions



Definitions to Note

- Conflict of Interest
- Conflict of Commitment
- Covered Individual
- Covered international travel and international travel
- Foreign government-sponsored talent recruitment program
- Insider Threat
- Research security incident
- United States Government support research and development

*....includes projects that **use U.S. Government equipment, facilities, or data** for conducting R&D.....*



Congress is losing patience with OSTP.

Source: [Why the White House is taking so long to issue new research security rules](#) | Science | AAAS



Integrated Research Security Program Requirements

Research Security Point of
Contact/Contact Information

Publicly available website
describing the program

Response to and reporting of
incidents of non-compliance

Regular self-assessments

Component Parts for Training Programs

- Foreign Travel Security
- Research Security Training
- Export Control Training
- Cybersecurity

Research Security Program



Foreign Travel Security

- Travel policy for Covered Individuals' organizational and sponsored travel
- Organizational record of travel
- Authorization and advance approval
- Mandatory security briefings
- Device security

Research Security Training

- RCR – initial and refresher (appropriate for the audience)
- Tailored training in response to incidents/findings
- Tracking of completion
- Threat awareness
- Insider threats
- Annual certification of training program

Export Controls Training

General Training

- Applicable laws
- Controlled items and technology
- Institutional policies
- Institutional contacts

Project Specific Training

- Specific restrictions
- Contract terms
- License terms and/or Technology Control Plan
- Disclosure of Information
- Shipping, if applicable





Cybersecurity

- Baseline safeguarding including protection from ransomware
- Protocols for storage, transmittal and conduct of FFR&D
- Limit access to authorized users
- Firewalls separating publicly available and internal systems
- Frequent updates
- Periodic scans
- Additional protections for classified, controlled unclassified, confidential information

Department of Defense Contracts

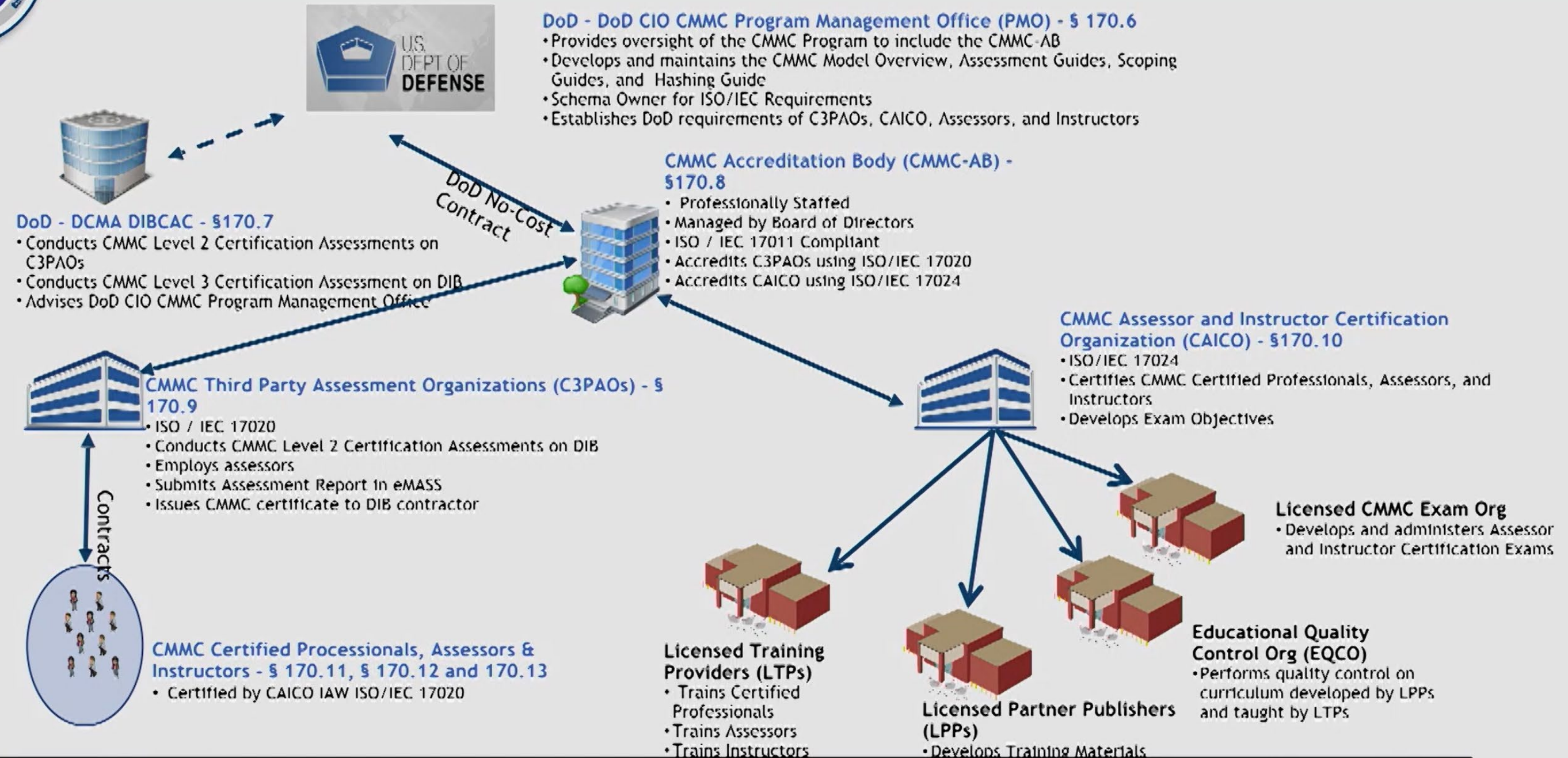
- DFARS 252.204-7000 Disclosure of Information (Oct 2016)
- DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Jan 2023)
- DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements (Jan 2023)
- NIST 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations





UNCLASSIFIED

The CMMC Ecosystem




International Organization for Standardization / International Electrotechnical Commission (ISO / IEC) 17011: *Conformity Assessment - Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies*
ISO / IEC 17020: *Conformity Assessment - Requirements for the Operation of Various Types of Bodies Performing Inspection*
ISO / IEC 17024: *Conformity Assessment - General Requirements for Bodies Operating Certification of Persons*

UNCLASSIFIED

So where did
your brain go
when you
heard
C3PA0?



Cybersecurity Maturity Model Certification (CMMC) Proposed Rule Overview

 **UNCLASSIFIED**

Implementation

- Program Codification (32 CFR) versus implementation (48 CFR) through DFARS 252.204-7021
 - Synchronization between the two rules
 - Schedule implications and constraints
- DFARS 252.204-7012 versus DFARS 252.204-7021
- CMMC will use a phased-in approach

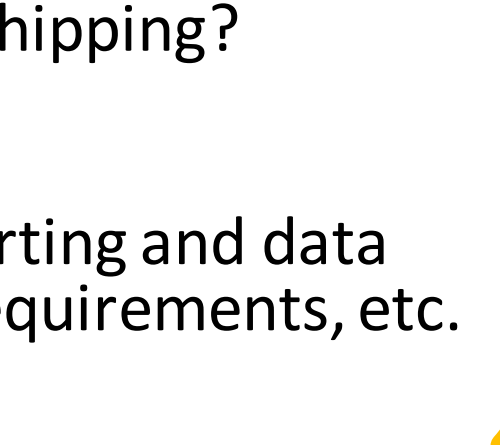
Phase 1	Phase 2	Phase 3	Phase 4 (Full Implementation)
Begins at Effective Date Where applicable, solicitations include Level 1 or 2 self-assessment Similar to existing DFARS 252.204-7020 requirement Some solicitations may require Level 2 certification	Begins 6 months later Where applicable, solicitations require Level 2 certification Some solicitations may require Level 3 Solicitation may specify the certification due at award or at option period	Begins 12 months later (18 months after effective date) Where applicable, solicitations include Level 1, 2, or 3 requirements For level 3 only, solicitation may specify due at option period (all others due at award)	12 months later (30 months after Effective Date) DoD intends all solicitations will include the applicable CMMC level requirement

- Government program managers and requiring activities may seek senior DoD executive approval to waive inclusion of the CMMC requirement.



International Collaborations

Assessing Risk: Foreign Subawards & Collaborations

- What does your award require?
 - Is it fundamental research?
 - Are there any export controls concerns including shipping?
 - Does it involve a country of concern?
 - Flow down and award requirements e.g. NIH reporting and data documentation requirements, research security requirements, etc.
 - [NIH FAQs Foreign Subawards](#)
- 

PROPOSED BIOSECURITY OVERSIGHT FRAMEWORK FOR THE FUTURE OF SCIENCE

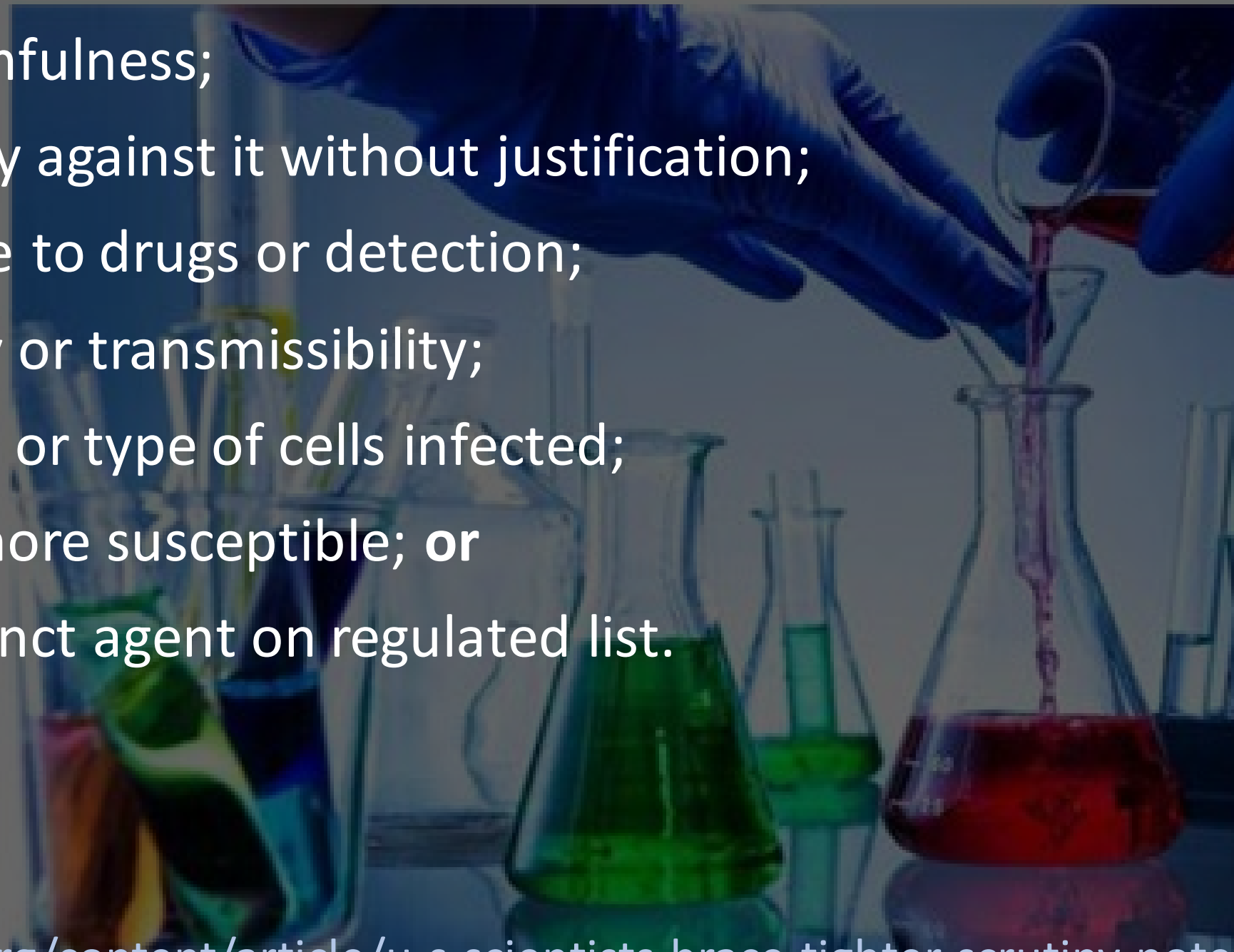
- Findings and recommendations from the National Science Advisory Board on Biosecurity (NSABB) – January 2023
- Questioned efficacy of DHHS Potential Pandemic Pathogen (PPP) Care and Oversight (P3CO) Policy
 - Roles for investigators and institutions
 - Expanded definition
- Stricter review of Dual Use Research of Concern (DURC)/enhanced potential pandemic pathogen (ePPP)
- Creation of a special office to help researchers comply

Retrieved from <https://osp.od.nih.gov/wp-content/uploads/2023/01/DRAFT-NSABB-WG-Report.pdf>

Additional references retrieve from <https://www.forbes.com/sites/stevensalzberg/2023/04/17/what-is-gain-of-function-research-and-why-should-it-be-banned/?sh=4bba59ed49dc> and <https://www.forbes.com/sites/stevensalzberg/2023/02/27/the-scientific-error-that-might-have-caused-the-covid-19-pandemic/?sh=30240c30341f>

Dual Use Research of Concern (DURC)

1. Enhance its harmfulness;
2. Disrupt immunity against it without justification;
3. Confer resistance to drugs or detection;
4. Increase stability or transmissibility;
5. Alter the species or type of cells infected;
6. Make the host more susceptible; **or**
7. Generate an extinct agent on regulated list.



Source: <https://www.science.org/content/article/u-s-scientists-brace-tighter-scrutiny-potentially-risky-research>

7 Elements of a Good Compliance Program

Established Policies, Procedures and Controls

Exercise Effective Compliance and Ethics Oversight

Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals

Communicate and Educate Employees on Compliance and Ethics Programs

Monitor and Audit Compliance and Ethics Programs for Effectiveness

Ensure Consistent Enforcement and Discipline of Violations

Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

Consequences of Violations

- Legal Implications
 - Civil: Fines and Forfeitures
 - Criminal: Fines and Incarceration
- Loss of Export Privileges
- Bad Press



Dealing with Potential Violations



Discovery

- Audits
- Provide a safe environment for reporting
- Have written procedures for handling potential violations



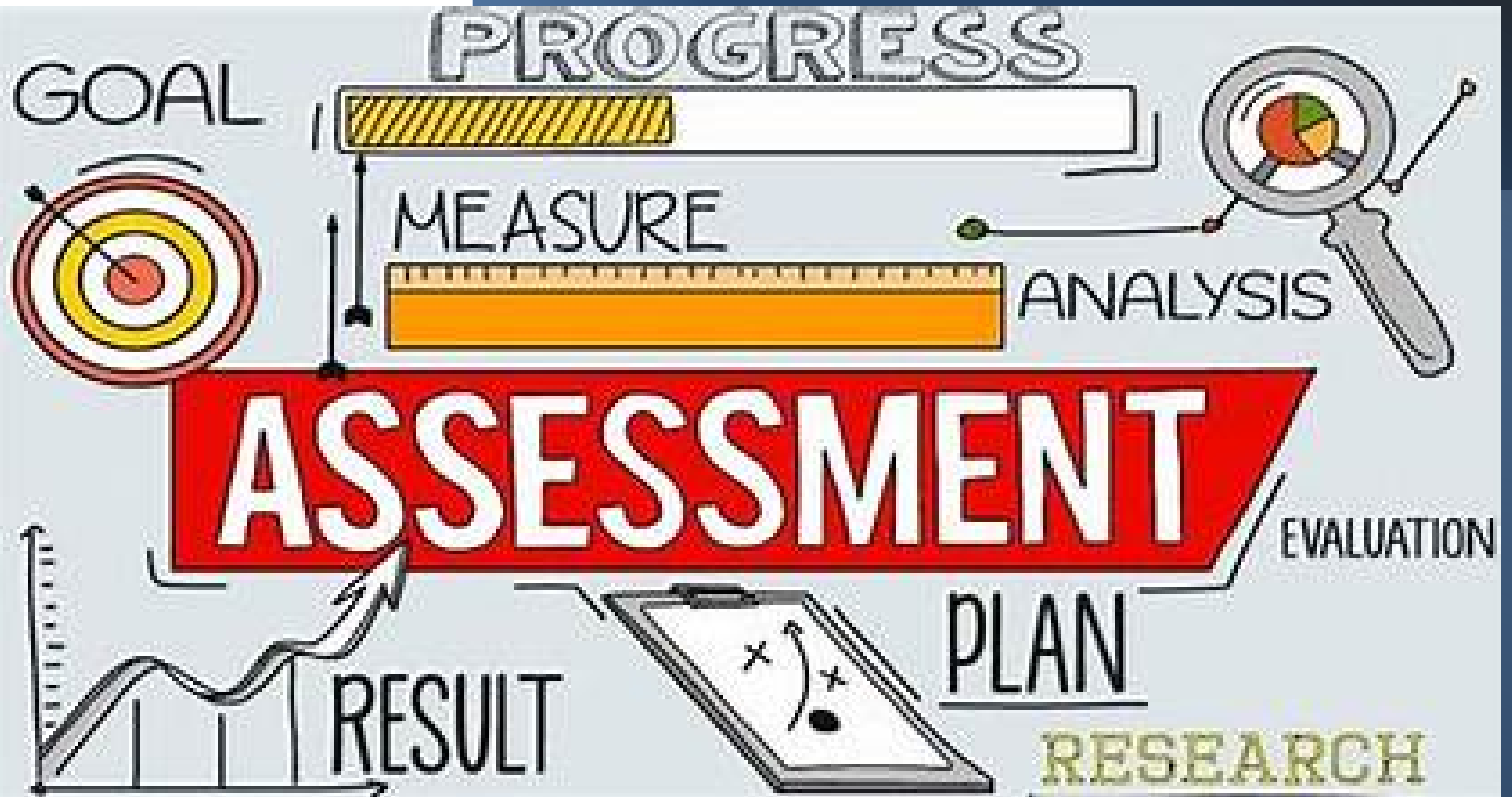
Investigation

- Provide a timely response
- Ensure compliance is restored
- Inform those on the escalation tree
- Self-report within required timeframe

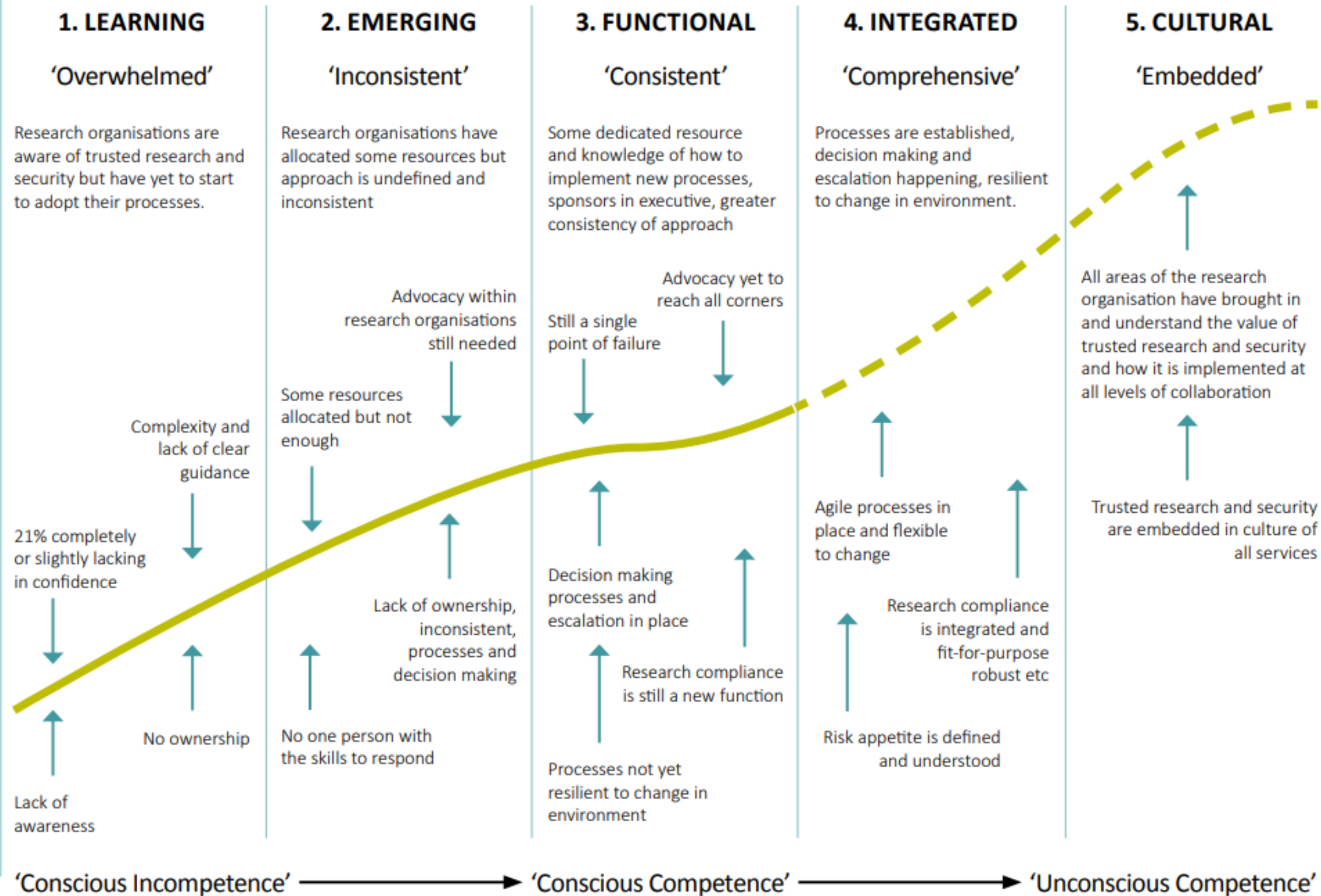


Corrective Action

- Determine the cause and accountability
- Revise internal controls, if needed
- Take disciplinary action, if warranted

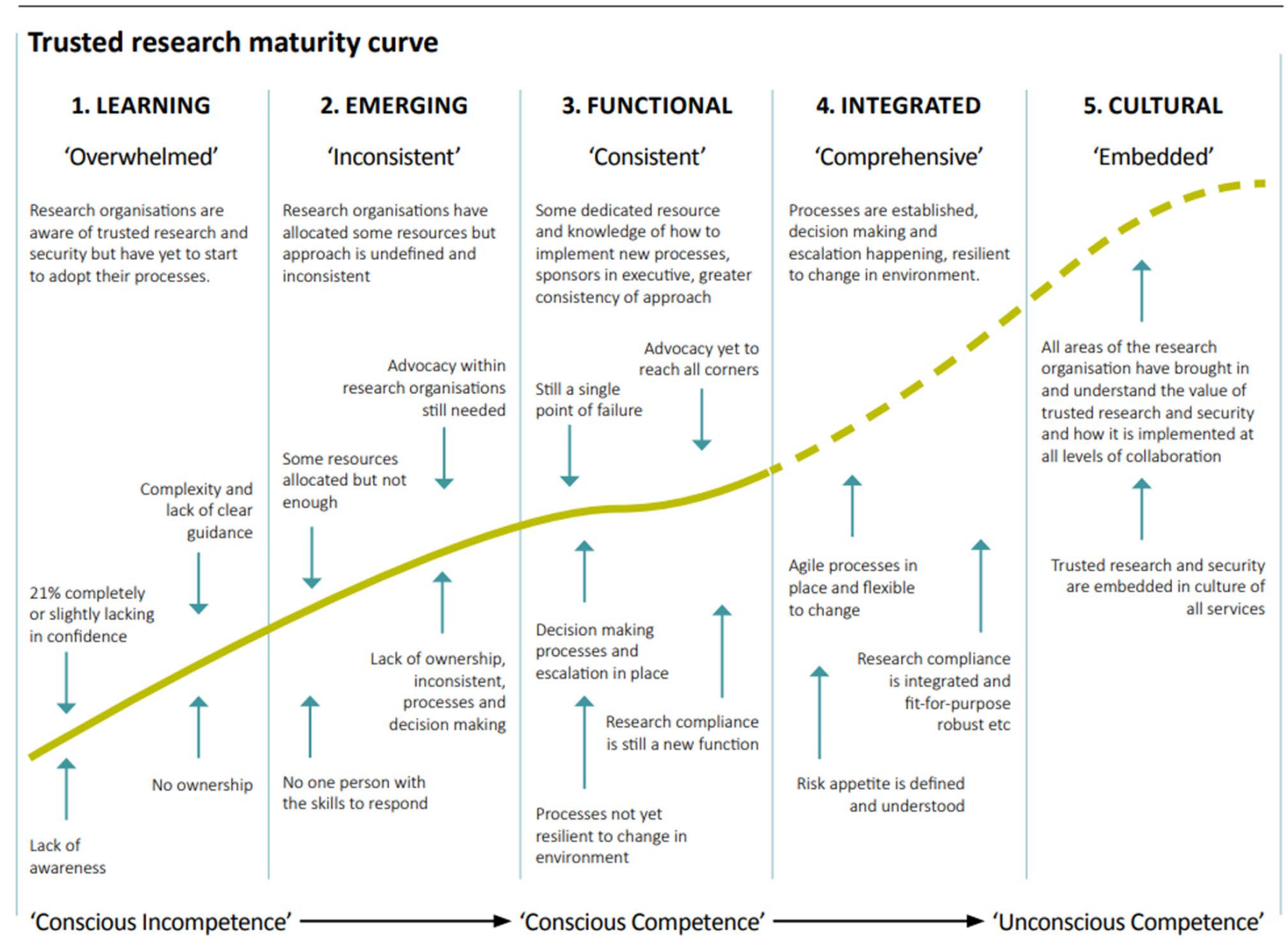


Trusted research maturity curve



Where is your organization?

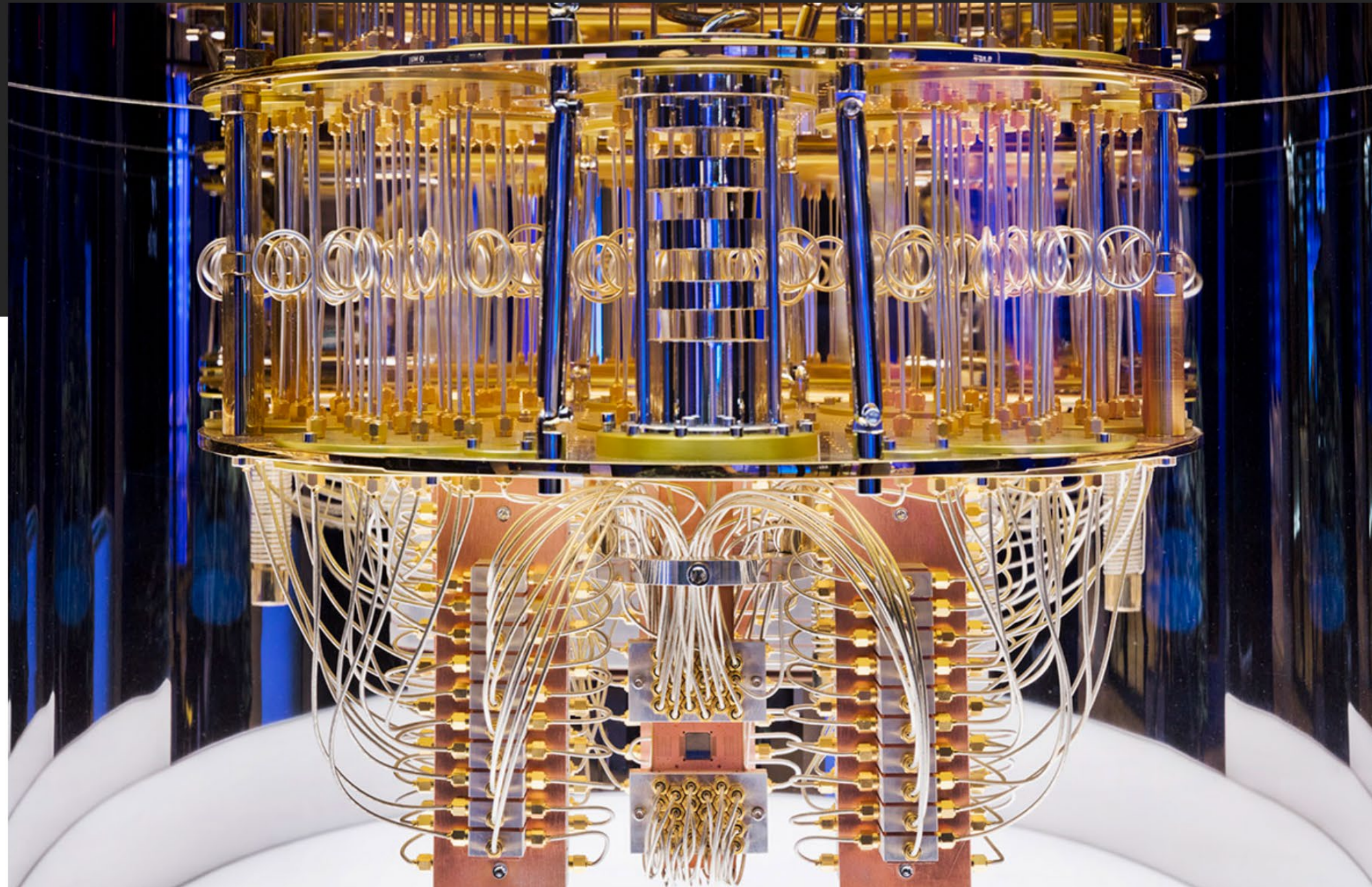
- Learning
- Emerging
- Functional
- Integrated
- Cultural



NSF tests ways to improve research security without disrupting peer review

Pilot follows recommendation to review each project rather than restricting topics

5 APR 2024 • 1:40 PM ET • BY [JEFFREY MERVIS](#)



Questions

Susan Wyatt Sedwick, PhD, CRA, CSM
ssedwick.ctr@attainpartners.com

➤ **Attain** Partners