NSF PDaSP: Towards Accelerating Use-Inspired and Translational Research in Privacy

NIST Workshop on Privacy Enhancing Cryptography

Sept 25, 2024

James Joshi
Program Director Expert
NSF Technology, Innovation and Partnerships (TIP) Directorate

(Professor, School of Computing and Information,
University of Pittsburgh)

Disclaimer: the presentation represents my views and interpretations

MISSION

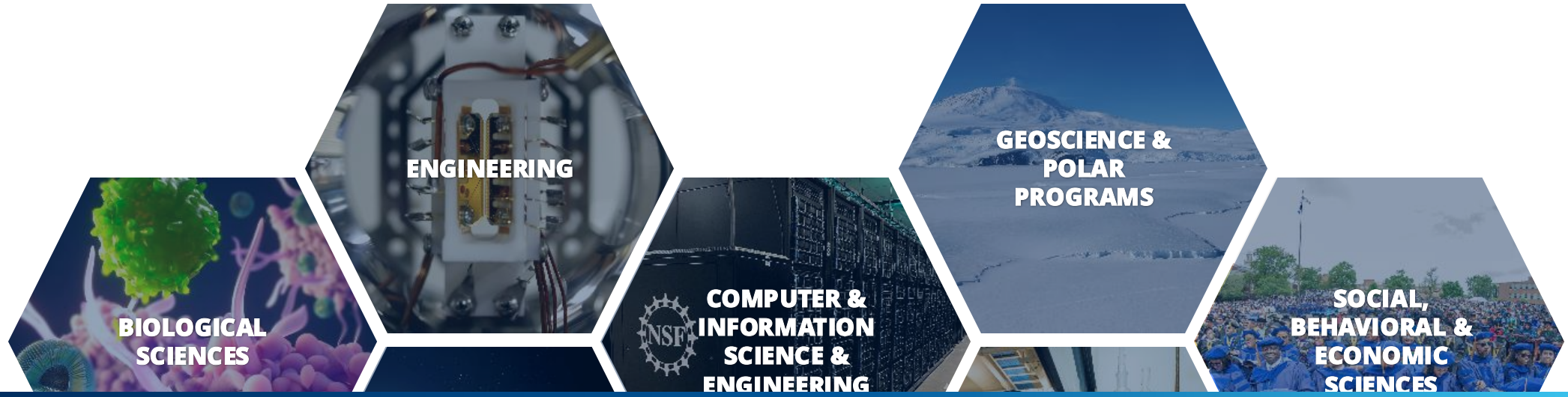
PROMOTE the progress of science

ADVANCE the national health, prosperity, and welfare

SECURE the national defense

NSF Supports Science & Engineering

U.S. National Science Foundation
Directorate for Technology, Innovation and Partnerships



DIRECTORATE FOR TECHNOLOGY, INNOVATION AND PARTNERSHIPS (TIP)

A new "horizontal" to enhance **use-inspired** and **translational** research

Established on March 16, 2022

Integrative Activities

International Science & Engineering


Artificial Intelligence
Advanced Communications and Wireless Technology
High-Performance Computing
Data and Cybersecurity
CHIPS & SCIENCE
10 KEY TECHNOLOGY AREAS
Quantum Information Science
Biotechnology
Robotics, Automation, and Advanced Manufacturing
Advanced Energy and Energy Efficiency
Resilience, Disaster Prevention, and Mitigation
Advanced Materials Science

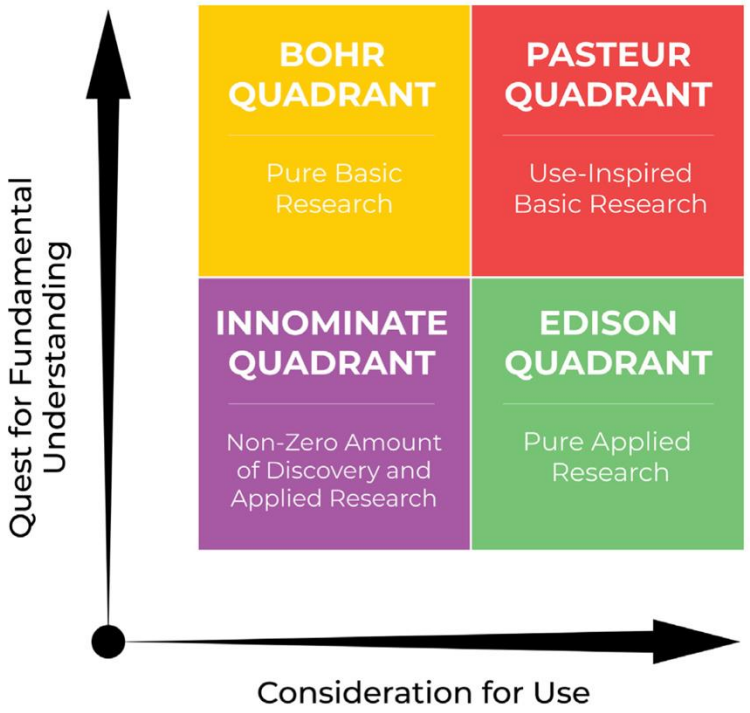
U.S. National Science Foundation
Directorate for Technology, Innovation and Partnerships

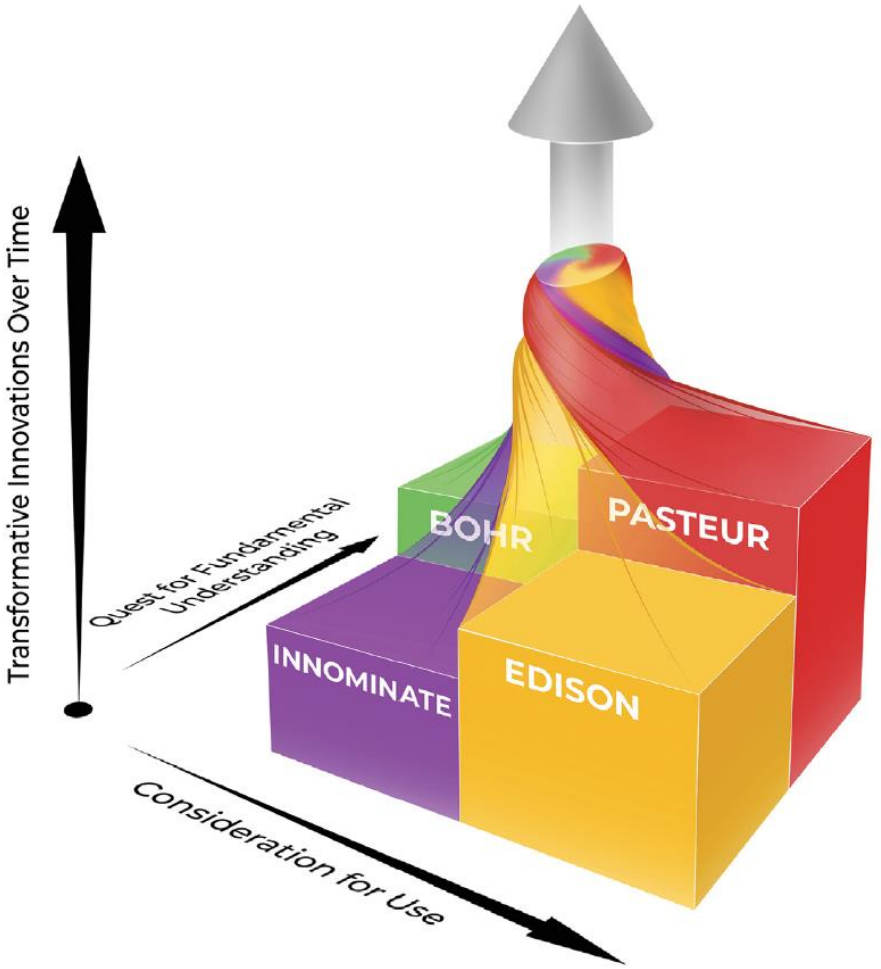
TIP Directorate Mission

TIP harnesses the nation's vast and diverse talent pool to advance critical and emerging technologies, address pressing societal and economic challenges, and accelerate the translation of research results from lab to market and society. TIP improves U.S. competitiveness, growing the U.S. economy and training a diverse workforce for future, high-wage jobs.

NSF Research support spans ..

- Foundational research
- Use-Inspired research
- Translational research
- …





Pettigrew & Cooke, "At the nexus of science, engineering, and medicine: Pasteur's quadrant reconsidered," 2022

TIP's Three Pillars

TIP advances U.S. competitiveness and societal impact by nurturing partnerships that drive and accelerate:

Diverse Innovation Ecosystems

Technology Translation and Development

Workforce Development

My NSF Experience

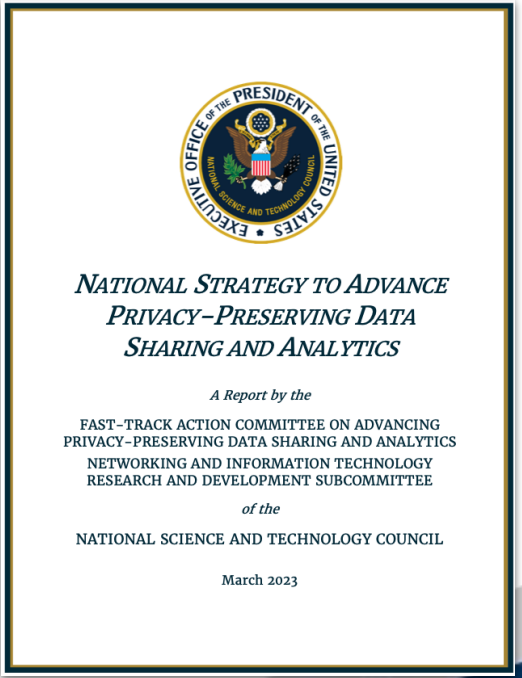
- Program Director (2019 – 2023)
  - CNS, Secure and Trustworthy Cyberspace SaTC) program
    - Mainly managing PRIVACY Portfolio
  - SaTC COVID Rapid lead/coordinator
    - 20+ SaTC RAPID Grants (many were Privacy related)
    - PREPARE Virtual Organization (Pandemic focused)
  - Co-Lead of US-UK PETs Prize Challenge (2022 – 2023)
    - With NIST and White House OSTP
    - Follow up of the Workshop: A Roadmap for Greater Public Use of Privacy-Sensitive Government Data: Workshop
  - FTAC Co-Chair:
    - National Strategy to Advance Privacy Preserving Data Sharing and Analytics (PPDSA)
    - National Strategy for Digital Assets R&D (paused)
  - Writing group member for:
    - Federal Cybersecurity R&D Strategy (Published in Dec, 2023)
    - National Privacy Research Strategy (ongoing)

Currently:
PD Expert at TIP

US-UK Privacy-Enhancing Technologies PRIZE CHALLENGE

Privacy Preserving Federated Learning
- **Financial Crime**
- **Pandemic Prediction**

Announced in the 2nd Summit for Democracy



PDaSP: Privacy Preserving Data Sharing in Practice

Launched on June 26, 2024

- **Goal**: Advance **privacy preserving data sharing and analytics** (PPDSA) technologies:
  - Fostering use-inspired and translational research *to accelerate transition to practice*
  - Maturing and scaling solutions to enable privacy-preserving data sharing
  - Promoting PPDSA technologies to derive value from data

PDaSP

$23M

- Multi-Industry + Multi-agency
- Within NSF: TIP & CISE (CNS, SaTC)
- Deadline: Sept 27, 2024

Aligns with: Executive Order on Safe, Secure, and Trustworthy Development and Use of AI

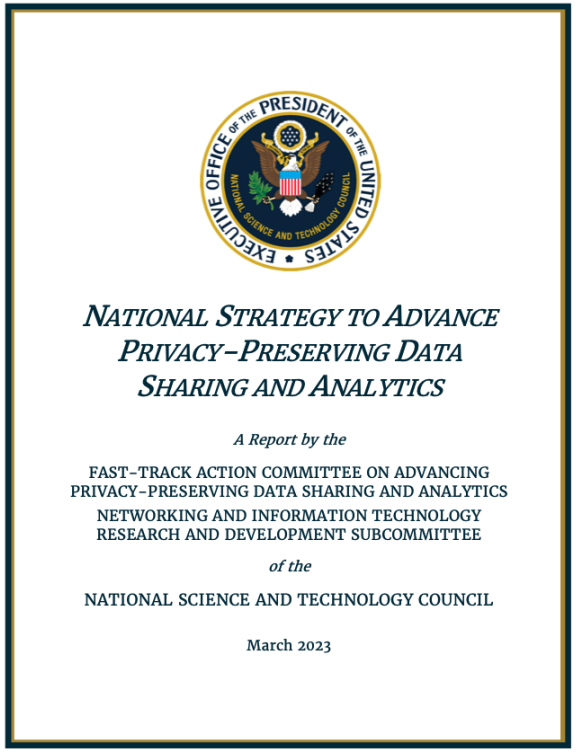
*The Director of NSF shall engage with agencies to identify ongoing work and potential opportunities to incorporate **PETs** into their operations. **The Director of NSF shall, where feasible and appropriate, prioritize research — including efforts to translate research discoveries into practical applications — that encourage the adoption of leading-edge PETs solutions for agencies' use**.*

(PETs: Privacy Enhancing Technologies)

in coordination with the Secretary of Commerce and Secretary of Energy: *developing and helping to **ensure the availability of testing environments, such as testbeds**, to support the development of safe, secure, and trustworthy AI technologies, as well as **to support the design, development, and deployment of associated PETs**.*

National Strategy to Advance PPDSA

- Strategic priority 3: Accelerate Transition to Practice
  - **Promote applied and translational research and systems development**
  - Accelerate efforts to develop standardized taxonomies, **tool repositories, measurement methods, benchmarking, and testbeds**
  - **Improve usability and inclusiveness of PPDSA solutions**



NATIONAL STRATEGY TO ADVANCE PRIVACY-PRESERVING DATA SHARING AND ANALYTICS

A Report by the

FAST-TRACK ACTION COMMITTEE ON ADVANCING PRIVACY-PRESERVING DATA SHARING AND ANALYTICS
NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT SUBCOMMITTEE

of the

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

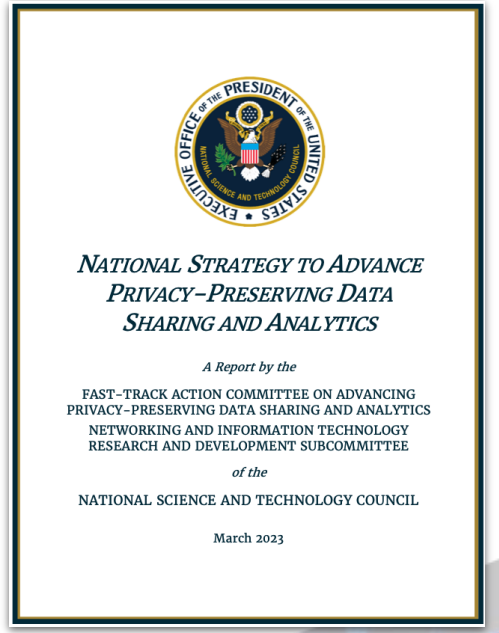
March 2023

The strategy also emphasizes public-private and international collaborations!

PDaSP Program

- Track 1: Advancing Key technologies to enable practical PPDSA solutions
  - $500K – $1M | Up to 12 Awards
- Track 2: Integrated and comprehensive solutions for trustworthy data sharing in application Settings
  - $1K – $1.5M | Up to 7 Awards
- Track 3: Usable tools and testbeds for trustworthy sharing of private or otherwise confidential data.
  - $500K – $1.5M | Up to 7 Awards

Aligns with:



Program Directors:

- TIP: Gail Joon-Ahn (Expert), James Joshi (Expert)
- CISE (CNS, SaTC): Anna Squicciarini, Cliff Wang

PDaSP Tracks

- **Track 1**: Advancing key technologies to enable practical PPDSA solutions
  - Mature individual PPDSA technology, or a combination of technologies for a specific use-case or application area
  - **Examples** (for illustration only!)
    - maturing homomorphic encryption to support privacy-preserving analytics over shared data; or
    - attribute-based encryption to enforce privacy-aware access control and data use policies to support a chosen application in an edge-cloud environment; or
    - combining a cryptographic technique (e.g., multi-party computation) with a statistical disclosure limitation technique (e.g., differential privacy) to enable privacy-preserving collaborative machine learning

Specific Privacy Enhancing Cryptography
- HE, FE, MPC/PSI, etc.

Anonymization and Statistical Disclosure Limitation techniques
..

PDaSP Tracks

- **Track 2**: Integrated and comprehensive solutions for trustworthy data sharing in application Settings
  - Focused on development of holistic system architectures that support end-to-end privacy protection and verifiable chain of trust
  - Should consider ecosystem challenges:
    - cross-organizational and cross-jurisdictional issues, economic incentives, etc.
  - Should tackle challenges related to specific use-cases and application contexts:
    - technological, regulatory/legal context, etc.

One technology that demonstrates significant promise for addressing end-to-end protection and the trade-offs between usability and verifiable privacy is ***Confidential Computing.***

- **Example(s)** (for illustration only!)
  - Using Confidential Computing for supporting advanced collaborative analytics that are compliant with privacy laws, e.g., considering: data-use policy enforcement, privacy-preserving analytics with end-to-end guarantees, etc.

PDaSP Tracks

- **Track 3**: Usable tools and testbeds for trustworthy sharing of private or otherwise confidential data
  - Address urgent need for effective/practical and easy-to-use *tools* and *testbeds* to lower the barrier for adoption of PPDSA solutions
  - Support privacy auditing, assess privacy disclosure risks, manage privacy parameters, improve trust and transparency, etc.
    - Enhance capabilities of all stakeholders
  - Emphasis is on testbeds that support assessment, comparative analysis, vulnerability or threat analysis, privacy risk assessments, and privacy-utility trade-off analysis.
  - Should include an application area or use-case that will serve as the demonstration for the effectiveness of the proposed tools and make the tool publicly available.
  - **Example(s)** (for illustration only!)
    - Sandboxed testing and assessment platforms for testing regulatory compliant PPDSA technologies for cross-border financial data sharing and analytics.

Partnership - Industry

- Intel Inc.
  - Co-funding and limited access to Confidential Computing resources - Software Guard Extensions (SGX) or Intel Trust Domain Extensions (TDX)
  - Will mainly support Track 2 proposals, in particular, those that use Confidential Computing
- VMware LLC
  - Co-funding mainly to Track 2 and Track 3 proposals
  - Will also consider proposals that focus on Confidential Computing and other PPDSA technologies that are relevant to AI Application

Partnership - Agencies

- U.S. Department of Transportation: Federal Highway Administration
  - Co-funding of projects in Tracks 1 and 2
  - Projects of interest would be that focused on *Naturalistic Traffic Studies in Privacy-Preserving Manner*
- U.S. National Institute of Standards & Technologies
  - Co-funding and sharing of testbed initially focused on privacy-preserving federated learning (PPFL)
  - Participants welcome to use the software platform or collaborate with NIST

Partner engagement

- **Pre-award**
  - Provide input to selected subset of proposals (after NSF review panels)
  - NSF makes final decisions by taking into consideration the inputs
- **Post award**
  - Participate in PDaSP PI meetings
  - A partner's researchers may directly participate in or collaborate with projects/PIs
- There is no IP sharing – Partners have agreed to "public dedication" to IP, publishing, and licensing

Looking Ahead

- Current plan is to continue PDaSP annually
- Broaden public-private partnership
- We welcome new partners
  - If you would like to explore/discuss, please reach out to one of us
    - Contact: James Joshi, jjoshi@nsf.gov
    - Or email: TIP-PDaSP-Ask@nsf.gov

Check out!

- Several other NSF programs emphasizing Privacy
  - **SaTC**: Secure and Trustworthy Cyberspace
  - **CICI**: Cybersecurity Innovation for Cyberinfrastructure
  - **Safe-OSE**: Safety, Security and Privacy of Open-Source Ecosystem
  - **IMR**: Internet Measurement Research: Methodologies, Tools, and Infrastructures
  - ….

PDaSP

- NSF PDaSP page: https://new.nsf.gov/funding/opportunities/privacy-preserving-data-sharing-practice-pdasp
- Recorded info session: https://new.nsf.gov/funding/opportunities/privacy-preserving-data-sharing-practice-pdasp/announcements/109295
- Also check out the TIP ROADMAP: https://nsf-gov-resources.nsf.gov/files/TIPRoadmap_WEB.pdf

And lastly .. TIP Roadmap

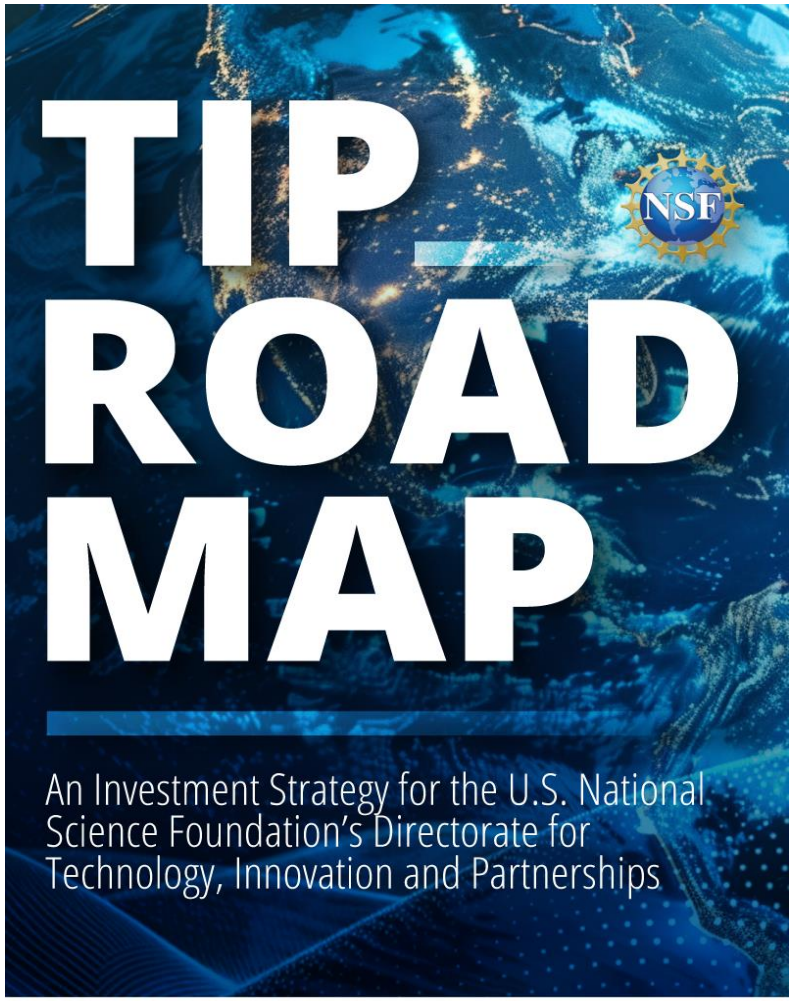
U.S. National Science Foundation
Directorate for Technology, Innovation and Partnerships

TIP Releases 2024 Investment Roadmap

An investment roadmap outlining the directorate's strategic vision that will, in turn, guide initial investment decisions focused on advancing U.S. competitiveness in key technology areas. Assessments of the key technology areas will be conducted every three years by updating the TIP roadmap, informing the directorate's plans for staging investments for maximal effect on U.S. competitiveness.

In the coming three-year window, TIP will focus on cultivating targeted investments to increase U.S. competitiveness in four primary key technology areas:

- *Artificial intelligence (AI), machine learning, autonomy, & related advances*
- *Biotechnology, medical technology, genomics, & synthetic biology*
- *Advanced communications technology & immersive technology*
- *Data storage, data management, distributed ledger technologies, & cybersecurity, including biometrics*



U.S. National Science Foundation
Directorate for Technology, Innovation and Partnerships

Learn more at:
https://new.nsf.gov/tip/updates/nsf-announces-investment-roadmap-technology

Thanks!

Questions?