PDaSP: Privacy-Preserving Data Sharing in Practice

$23M

DEPARTMENT OF TRANSPORTATION
UNITED STATES OF AMERICA

NIST

Information Session

July 23, 2024

intel®

vmware® by Broadcom

Agenda

- Introductions
- Welcome Message from TIP Leadership
- PDaSP Program Overview
  - Program Goals
  - Tracks
  - Partners
  - Eligibility
  - Evaluation criteria
  - Miscellaneous
- Q/A Session

The National Science Foundation's mission

"To promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense..."

2021

NSF’s existing directorates and offices (till 2022)

Biological Sciences

Engineering

Mathematical & Physical Sciences

Computer & Information Science & Engineering

Geosciences (including Polar Programs)

Integrative Activities

Education & Human Resources

Social, Behavioral & Economic Sciences

International Science & Engineering

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

Engineering
Geosciences (including Polar Programs)
Social, Behavioral & Economic Sciences
Biological
Computer & Information
Education &
Mathematical & Physical Sciences
Integrative Activities
International Science & Engineering

DIRECTORATE FOR TECHNOLOGY, INNOVATION AND PARTNERSHIPS (TIP)

March 16, 2022: NSF establishes TIP

Welcome Remarks

Graciela Narcho

Deputy Assistant Director

Directorate for Technology, Innovation and Partnerships (TIP)

National Science Foundation

NSF – TIP and CISE

- **PDAsP** Program is a partnership-based initiative
  - NSF Units
    - **TIP Directorate** – *Innovation & Technology Ecosystems* (ITE) Division
      - **Program Director Expert**: James Joshi
    - **CISE** - *Computer and Network Systems* (CNS) Division & *Secure and Trustworthy Cyberspace* (SaTC) program
      - **Program Directors**: Anna Squicciarini, Cliff Wang
  - Partnership with Industry and other federal agencies (**more later**)
    - Intel, VMware
    - DoT FHWA, NIST

Program Goals

- Advance **privacy preserving data sharing and analytics** (PPDSA) technologies to enable a trustworthy and accountable data driven future and create the foundation for responsible open science and scientific innovation by:
  - Fostering use-inspired and translational research to advance innovative models, methodologies, or constructs
  - Maturing and scaling solutions at the intersection of privacy goals and socio-economic or policy challenges
  - Leveraging both hardware and software foundations to enable individuals and organizations to derive value from the data in a manner that preserves privacy and reinforces accountability

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

WH.GOV

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

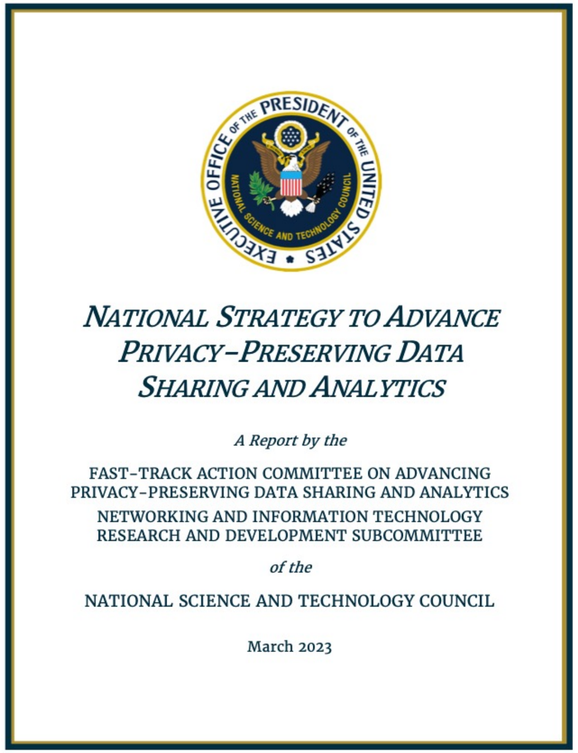
*The Director of NSF shall engage with agencies to identify ongoing work and potential opportunities to incorporate **PETs** into their operations. **The Director of NSF shall, where feasible and appropriate, prioritize research — including efforts to translate research discoveries into practical applications — 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 testbed**s, 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

- Seeks to foster innovative, use-inspired and translational research to mature and scale existing models, methodologies, or constructs in order to accelerate the development and deployment of practical privacy-preserving data sharing solutions.

Privacy-Preserving Data Sharing in Practice (PDaSP)

View guidelines

NSF 24-585

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

Some important things to keep in mind

- Relevant expertise
- Clear threat models or risks and harms
- Practical privacy-utility

Up to 12 awards

Budget range: $500K - $1M for upto 2 years

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.

Some important things to keep in mind
- Relevant expertise
- Clear threat models or risks and harms
- Practical privacy-utility

Up to 7 awards

Budget range: $1M - $1.5M for up to 3 years

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.

Important things to keep in mind

- Relevant expertise
- Clear threat models or risks and harms
- Practical privacy-utility

Up to 7 awards

Budget range: $500K - $1.5M for up to 2 years

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
  - Access to CC resources will be mainly for track 2, but also for other tracks where the need is well articulated

Partnership - Industry

- 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*
  - FHWA requires a minimum 20 percent funding match for the FHWA portion of funding
    - In kind based on the value of equipment, materials, data, or labor
    - This requirement will **not** be included as a condition of the NSF award

Partnership - Agencies

- U.S. National Institute of Standards & Technologies
  - Currently building PETs testbed initially focused on privacy-preserving federated learning (PPFL)
    - open-source software to run locally and in a cloud environment that simulates a central server connected to a set of data silos.
    - initial deployment focuses on genomic data and providing input and output privacy protections.
  - Participants welcome to use the software platform or collaborate with NIST

Partners 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

New Partners may join by the deadline of August 27 –
So please check back and plan accordingly!

Quick break for Q/A on topics so far

Eligibility – Who may submit?

- **Institutions of Higher Education** (IHEs) - **Two- and four-year IHEs** (including community colleges) accredited in, and having a campus **located in the U.S.,** acting on behalf of their faculty members.
- **Non-profit, non-academic organizations**: Independent museums, observatories, research laboratories, professional societies and **similar organizations located in the U.S.** that are directly associated with educational or research activities.
- **U.S.-based small businesses**, as defined by SBA's small business size regulations 13 CFR Part 121, with strong capabilities in scientific or engineering research or education and a passion for innovation.

No limit on number of proposals from each institution !!

Eligibility – Who may serve as PI?

- The PI, co-PIs, or any other senior/key personnel **must hold an appointment at an organization that is eligible** to submit as described under "Who May Submit Proposals."
- Researchers with primary appointments at overseas branch campuses of U.S. institutions of higher education are **not** eligible.
- Researchers from foreign academic institutions who contribute essential expertise to the project may participate as senior/key personnel or collaborators but may not receive NSF support.
- Individuals **affiliated with a partner** involved in this solicitation, notably those who are currently employed by, consulting for, or on an active agreement to provide services for the partner, may **NOT** participate in proposals to the program.

Limit of 2 proposals per PI/Co-PI/key personnel

First TWO considered!

Proposal Evaluation

- **NSF Merit Review criteria**
  - **Intellectual Merit**: The IM criterion encompasses the potential to advance knowledge; and
  - **Broader Impacts**: The BI criterion encompasses the potential to benefit society and contribute to the achievement of specific, desired societal outcomes.
- **Additional Solicitation Specific Review Criteria**
  - For each track
  - Helps
    - Protect write effective proposals, and
    - Makes proposal review/evaluation easier

Proposal Evaluation – Track 1

- **Additional Solicitation Specific Review Criteria**
  - Does the proposal address a **significant translational research gap** in transitioning **theory to practice** for the key PPDSA technique(s) considered?
  - Do the expected outcomes **show promise of broader deployment or adoption of the PPDSA solution(s)** proposed considering factors such as scalability, efficiency, and privacy-utility trade-offs, as appropriate, for the identified use-cases or applications, while addressing practically relevant threat models?
  - Are the expected outcomes easily **generalizable, or customizable** to use-cases or applications not specifically considered in the proposal?
  - Does the project plan **adequately address system development and implementation milestones and evaluation**? Does the project team include **appropriate expertise** to ensure success of the project? As applicable, the project plan should include clear description of collaboration with any partnering organizations that would act as data provider, use-case provider, and/or early adopter.

Proposal Evaluation – Track 2

- **Additional Solicitation Specific Review Criteria**
  - Does the proposal address a **significant translational research gap** in transitioning theory to practice considering an **integrative, systems approach and end-to-end privacy protection**?
  - Does the proposal comprehensively address the challenges of privacy preserving data sharing and use **within specific data sharing community context, or application, considering the needs of all stakeholders, and relevant threat models**?
  - Does the proposal adequately **justify the practical challenges of integrating** various technologies across computing stack (i.e., they are not trivial) to enable privacy-preserving data sharing?
  - Is the integrated solution **justifiably more scalable, and more mature than comparable existing solutions**, or does the proposal demonstrate significant **promise for increased adoption or deployment** of the proposed integrative solution?
  - Does the **project plan adequately address system development and implementation milestones and evaluation**? Does the project team include appropriate expertise to ensure success of the project? As applicable, the project plan should include clear description of collaboration with any partnering organizations that would act as data provider, use-case provider, and/or early adopter.

Proposal Evaluation – Track 3

- **Additional Solicitation Specific Review Criteria**
  - Does the proposal adequately justify that the proposed **tools and/or testbeds are novel**, show promise to fulfill a **significant need**, and help **promote** PPDSA adoption?
  - Are the proposed tools **easy to use and deployable**, or can they be **easily integrated** in targeted system environments?
  - Does the proposed testbed show promise for **effectively supporting experimentation, testing and evaluation**, and/or **validation of PPDSA solutions**? Is the proposed testbed applicable for **a specific set of PPDSA solutions, data sharing communities or applications**, or are they **generalized**?
  - Is there a clear and **convincing plan for integrating and/or sustaining** the proposed tools or and testbeds within the broader PPDSA ecosystem (e.g., in open-source ecosystems).

Post Award

- **PI Meetings**
  - Kick-off meeting in Fall 2025
  - Annual PI meeting
  - At least one member must attend (include travel budget items for this travel)

- **Reporting requirements as per general NSF policy**
  - Annual reports
  - Final report

Miscellaneous

- Key Contacts:
  - James Joshi, TIP/ITE, telephone: (703) 292-8450, email: jjoshi@nsf.gov
  - Anna Squicciarini, CISE/CNS, telephone: (703) 292-5177, email: asquicci@nsf.gov
  - Xiaogang (Cliff) Wang, CISE/CNS, telephone: (703) 292-2812, email: xiawang@nsf.gov

Please contact NSF PDs for any questions!!

For questions regarding this program please email:
TIP-PDaSP-Ask@nsf.gov

Thanks!

Q/A Session