Research Security & Risk Management

Moderator: Dr. Mahesh Mani, Technical Program Manager
Office of Advanced Manufacturing, NIST

Timothy R. Wood Export Controls Program Manager Laboratory Programs, NIST Martin Stanley
Senior Advisor for Risk Management
Information Technology Laboratory, NIST





Artificial Intelligence Risk Management Framework (AI RMF 1.0)



WHAT IS THE AI RMF?



Voluntary resource for organizations designing, developing, deploying, or using AI systems to manage AI risks and promote trustworthy and responsible Al

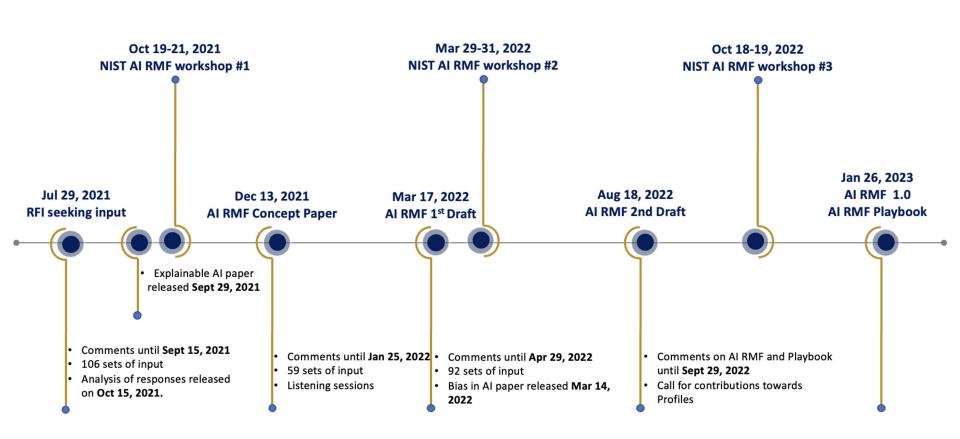
Rights-preserving

Flexibly Applied

Measurable

THE PATH TO AI RMF 1.0





KEY TERMINOLOGY



- Al systems: engineered or machine-based system that generates outputs such as predictions, recommendations, or decisions influencing real or virtual environments and operating with varying levels of autonomy.
- Risk: composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event.
 The impacts, or consequences, of AI systems can be positive, negative, or both and can result in opportunities or threats.

AI RISKS AND TRUSTWORTHINESS



Safe Secure & Explainable & Privacy-Enhanced Fair - With Harmful Bias Managed Accountable & Transparent Valid & Reliable

AI RISK MANAGEMENT





Risk measurement



Risk tolerance

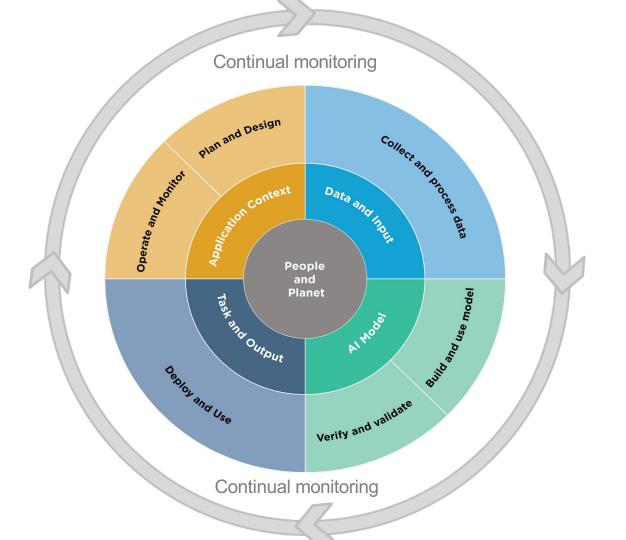


Risk prioritization



Risk integration & management

AUDIENCE: AI LIFECYCLE AND AI ACTORS



AI RMF CORE







NIST AI RMF Playbook

The Playbook provides suggested actions for achieving the outcomes laid out in the <u>AI Risk Management Framework</u> (AI RMF) <u>Core (Tables 1–4 in AI RMF 1.0)</u>. Suggestions are aligned to each sub-category within the four AI RMF functions (Govern, Map, Measure, Manage).

The Playbook is neither a checklist nor set of steps to be followed in its entirety.

Playbook suggestions are voluntary. Organizations may utilize this information by borrowing as many – or as few – suggestions as apply to their industry use case or interests.

Govern Map Measure Manage



Download the NIST AI RMF Playbook

Playbook PDF

Playbook CSV

Playbook Excel

Playbook JSON

AI RMF PROFILES

Implementations of the AI RMF functions, categories, and subcategories for a specific setting or application based on the requirements, risk tolerance, and resources of the Framework user.



Use-case profiles; e.g., hiring or fair housing



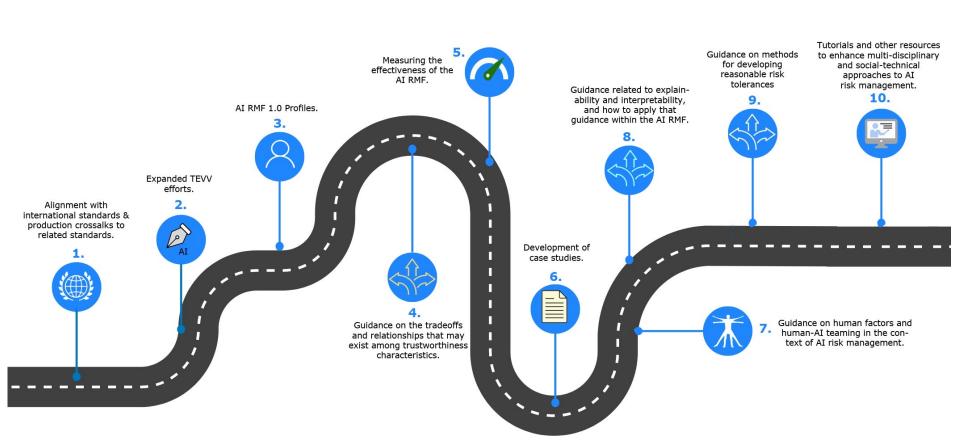
Temporal profiles; e.g., current state vs. the target state



Cross-sectoral profiles; e.g., large language models, cloud-based services or acquisition

What's next?





NIST TRUSTWORTHY AND RESPONSIBLE AI RESOURCE CENTER

NST

https://airc.nist.gov/







AI RMF PROFILES



AI RISK GLOSSARY



AI STANDARDS TRACKER



AI METRICS HUB



FOR MORE INFORMATION...





www.nist.gov/itl/ai-risk-management-framework

https://airc.nist.gov/



Alframework@nist.gov

Federal Al Landscape

Moderator: Mojdeh Bahar
Associate Director for Innovation & Industry Services, NIST

Elham Tabassi
Associate Director for Emerging Technologies
Information Technology Laboratory, NIST

Edwina Manyeh
Tech Hubs Deputy Director
U.S. Economic Development Administration

Dr. Bruce Kramer
Program Director
National Science Foundation





Al Innovation Lab

Elham Tabassi, Chief Al Advisor



NIST's Mission



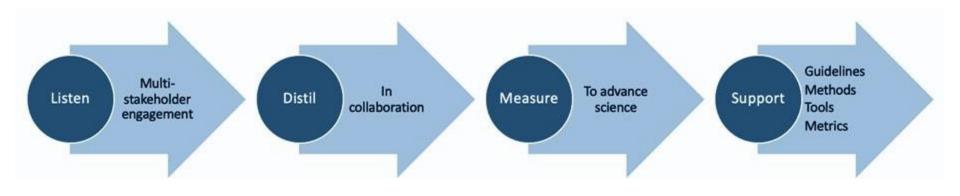
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life







NIST helps industry develop valid, scientifically rigorous methods, metrics and standards.



NIST AI Risk Management Framework and Resources NIST AI Risk Management Framework and Resources





NIST AI RMF: A voluntary resource for organizations designing, developing, deploying, or using AI systems to manage AI risks and promote trustworthy and responsible AI



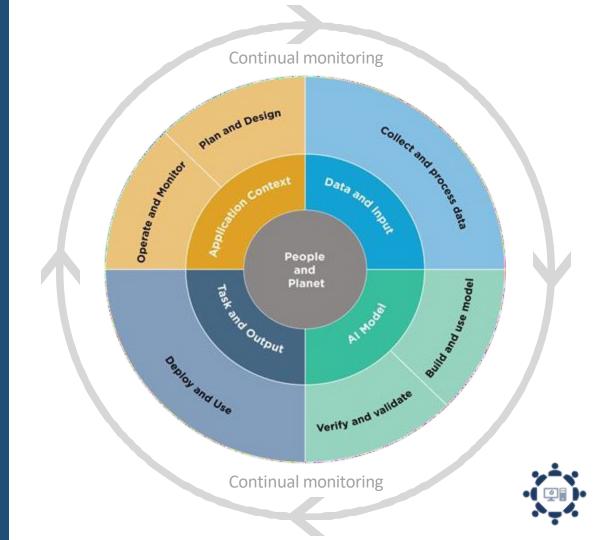


Al system trustworthiness can be defined in terms of well-understood characteristics.





Beyond the system, a culture of responsible practice and use must pervade activities across the entire Al lifecycle.



Major Achievements and Announcements Since 2023



NIST Due Dates Under Executive Order 14110

Submit report on synthetic content authentication to OMB and NSC	 Publish AI RMF for GAI Publish Secure Software Framework for GAI and dualuse models 	 Publish guidelines on the efficacy of differential- privacy-guarantee protections 	 Publish guidance for synthetic content authentication 	
June 26, 2024	July 26, 2024	October 29, 2024	December 24, 2024	January 26, 2025
	 Launch initiative to create guidance/benchmarks for evaluating and auditing Al capabilities Provide test environments Publish red-teaming guidelines Initiate engagement with industry and relevant synthetic nucleic acid sequence providers Publish synthetic content authentication report Publish a plan for global engagement on promoting and 			Submit a report to the President on priority actions taken pursuant to the Global engagement on standards plan

Artificial Intelligence Safety Institute Consortium (AISIC)

AISIC brings more than 280 leading AI stakeholders together to develop science-based and empirically backed guidelines and standards for AI measurement and policy, laying the foundation for AI safety across the world.

AISIC working groups sustain, scale, and implement E.O. elements

Risk Management for Generative Al

Synthetic Content

Capability Evaluations

Red-Teaming

Safety & Security



Team: Reva Schwartz (Lead)

Jonathan Fiscus, Kristen K. Greene, Craig Greenberg, Afzal Godil, Kyra Yee, Razvan Amironesei, Theodore Jensen (Feds)

Rumman Chowdhury (associate), Gabriella Waters (PREP), Patrick Hall (associate), Shomik Jain (pathway),



Evaluating Generative AI Technologies

A NIST evaluation program to support research in Generative AI technologies.





Team: Yooyoung Lee (Lead)

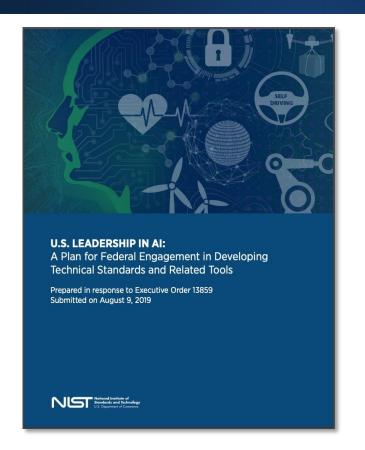
George Awad, Kay Peterson, Peter Fontana (Feds)

Lowen DiPaula (pathway student),

Seungmin Seo (associate)

USG AI Standards Coordinator









NIST works across government and with industry to identify critical standards development activities, strategies, and gaps



NIST is coordinating in part through the Interagency Committee on Standards Policy (ICSP) AI Standards Coordination Working Group

Global Engagements





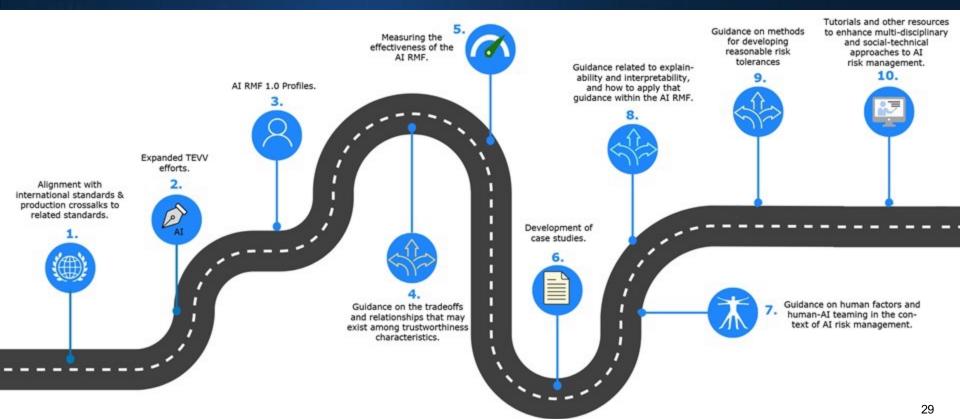








A roadmap of future work was released along with the AI RMF in January.



NATIONAL ARTIFICIAL INTELLIGENCE ADVISORY COMMITTEE (NAIAC)

The National Artificial Intelligence Advisory Committee (NAIAC) advises the President and the White House on the intersection of AI and innovation, competition, societal issues, the economy, law, international relations, and other critical areas.

Since first convening in May 2022

- ► 70+ experts interviewed across 26 public sessions
- ▶ 18 Recommendation reports/memos
- 6 Findings, including explainer documents and FAQs
- 2 Committee Statements
- 2 Annual Reports

The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence operationalized many of NAIAC's recommendations.

WHAT'S AHEAD

NAIAC will continue to offer recommendations and insights as a committee, in public stakeholder panels and in the activity across five working groups:

Al Education & Awareness International Collaboration Al Futures - Preparedness, Opportunities, and Competitiveness Safety, Trust, and Rights Al in Work and the Workforce

Additionally, the NAIAC Subcommittee on Al and Law Enforcement has introduced three distinct working groups:

Performance, Evaluation and Bias; Processes; Identification and Surveillance Set



Click, Connect, Collaborate!



www.nist.gov/itl/ai-risk-management-framework

airc.nist.gov

ai-challenges.nist.gov

ai.gov/naiac



AlFramework@nist.gov ai-inquiries@nist.gov



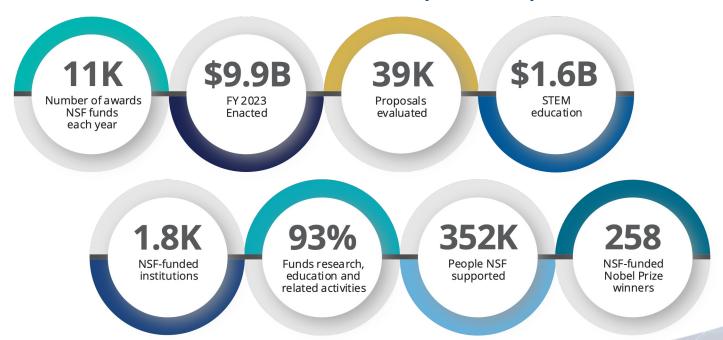
National Science Foundation Al Initiatives

NIST AI for Resilient Manufacturing USA Institute Proposers Day

> Gaithersburg, Maryland August 20, 2024

Bruce Kramer Senior Advisor, ENG/CMMI

NSF Vision: A nation that leads the world in science and engineering innovation, to the benefit of all, without barriers to participation





Leveraging NSF Programs

- **NSF 24-014** DCL: Advancing Fundamental Research and Education in Advanced Manufacturing with the Objectives of the Manufacturing USA Institutes. \$35M since 2017.
- **NSF 24-525**: Future Manufacturing, \$100M+ since 2020.
- NSF 21-598: Advanced Technological Education (ATE)
 Program world class technician education. National Applied
 Artificial Intelligence Consortium (NAAIC), Miami Dade
 College, \$2.8M, August 2024.
- **NSF 21-013**: INTERN Program Graduate-level internships in your Institute or member companies.

The National Artificial Intelligence Research Resource (NAIRR)

- Aims to implement a shared national research infrastructure for responsible discovery and innovation in AI, https://nairrpilot.org/.
 - Presidential Executive Order 14110 on Safe, Secure and Trustworthy Development and Use of Al, October 2023.
 - Spur Innovation, Increase Diversity of Talent, Improve Capacity, and Advance Trustworthy AI.
 - 13 Agencies + 25 companies including Amazon, AMD, Google, HP, IBM, Intel, Meta, Microsoft, NVIDIA, OpenAI, and Palantir.



National Al Research Institutes, NSF 23-610.

- \$20M (~4M/year) over 5 years
- Foundational and use-inspired Al research
- Innovation in Al education and workforce development
- New partnership development

Al Institutes and Funding Partners





A network of networks



Facilitator and Resource Center

- Directory of Institute contacts
- Advice on partnership inquiries

Learn more about Al Institutes at https://aiinstitutes.or



25 Active Institutes

- 2020: First cohort of Institutes (5 NSF, 2 USDA/NIFA)
- 2021: Second cohort of Institutes (9 NSF, 2 USDA/NIFA)
- 2023: Third cohort of Institutes (6 NSF, 1 USAD/NIFA)

AIVO: https://aiinstitutes.org
Link to all awards: NSF Award
Search











ATHENA ALINSTITUTE











































NSF-led National AI Research Institutes Program



7 Institutes

3 Funding Partners

DHS, USDA/NIFA

Tracks

- Trustworthy AI
- Foundations of Machine Learning
- Al-Driven Innovation in Agriculture and the Food System
- Al-Augmented Learning
- Al for Accelerating Molecular Synthesis and Manufacturing
- Al for Discovery in Physics



11 Institutes

5 Funding Partners

DHS, USDA/NIFA, Accenture, Amazon, Google, Intel

Tracks

- Human-Al Interaction and Collaboration
- Al for Advances in Optimization
- Al and Advanced Cyberinfrastructure
- Al in Computer and Network Systems
- Al in Dynamic Systems
- Al-Augmented Learning
- Al-Driven Innovation in Agriculture and the Food System



7 Institutes5 Funding Partners

DHS, DOD, Education, NIST, USDA/NIFA, IBM

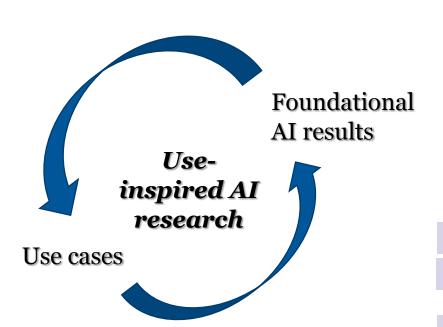
Tracks

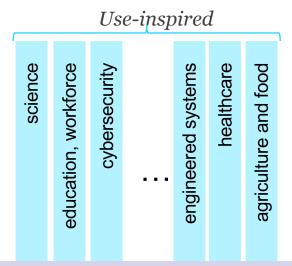
- Intelligent Agents for Next-Generation Cybersecurity
- Neural and Cognitive Foundations of Artificial Intelligence.
- Climate Smart Agriculture and Forestry
- Al for Decision Making
- Trustworthy AI
- Al-Augmented Learning to Expand Education Opportunities and Improve Outcomes





Foundational and Use-Inspired AI Research





learning, abstraction, and inference

reasoning, uncertainty, causality

agents and multiagent systems

Al architectures, multi-strategy Al,



Trustworthy AI for Supply Chains



challenges

new realities and expectations demand a new vision

- lack of downward/upward visibility
- volatility of just-in-time systems
- environmental impact of e-commerce
- lack of synchronization with manufacturing
- disparate service levels







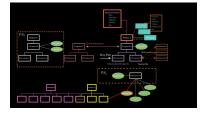
a new vision

- end-to-end modeling and optimization
- managing risk and volatility
- integrating supply chains and manufacturing
- eliminating waste through reverse supply chains
- designing fair supply chains





end-to-end optimization

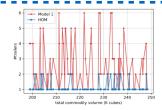


at scale

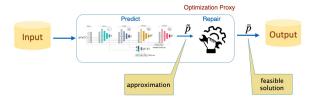


with real-time risk assessment





downstream/upstream forecasting



real-time optimization by fusing AI and OR



explanations for planners/operators













What to do

- NSF Award Search: find university-based partners, https://www.nsf.gov/awardsearch/.
- Create a formal protocol for working with colleges and universities.
 - NSF 23-054 DCL: Research on Integrated Photonics Utilizing AIM Photonics Capabilities is a good model.
- Propose a National Artificial Intelligence Research Institute, NSF 23-610.

Your University Members Know NSF's Programs!











Tech Hubs Program Overview

Edwina Manyeh
Tech Hubs Deputy Director

August 20, 2024

Tech Hubs Vision

The Tech Hubs Program aims to strengthen U.S. economic and national security by investing in geographically diverse regions across the country with the potential to become globally competitive in the next decade to ensure the technologies, industries, and jobs of the future start, grow, and remain in the United States.



Tech Hubs Funding

LEGISLATION FUNDING Authorization CHIPS and Science Act \$10 billion \$500 million FY 2023 Omnibus \$541 million **Appropriations** appropriated FY 2024 Consolidated \$41 million **Appropriations Act**



What is a Tech Hub?

 Tech Hubs Designation is an endorsement of a Tech Hub's plans to supercharge its technology industry, create jobs, and strengthen U.S. economic and national security.



Regional Ecosystem



Core Technology Area



Commercial Leadership Potential





Investing in Tomorrow

The U.S. government has vetted Tech Hubs' project portfolios and endorses Designees as strong candidates for investment. We believe each Hub will:

0

Strengthen U.S. economic security

2

Strengthen U.S. national security

3

Have the potential to become **globally competitive** in the next decade

4

Ensure the technologies, industries, and jobs of the future start, grow, and remain in the U.S.





Regional Investment, Global Opportunity

Through regional, place-based investments, Tech Hubs are equipped to deliver scaled global production in these critical technological areas:



Autonomous Systems (3)



Maintaining Our **Quantum Edge** (2)



Advancing **Biotechnology**: Drugs and Devices (6)



Advancing **Biotechnology**: Precision and Prediction (5)



Accelerating Our **Energy Transition** (5)



Regaining Leadership in **Semiconductor** Manufacturing (4)



Strengthening Our Critical
Minerals Supply Chain (2)



Growing the Future of **Materials Manufacturing** (4)





Our Program



Geographic Reach

- 45 States + Puerto Rico
- 640 Counties
- States Served
- Safe and Effective
 Autonomous Systems
- Maintaining Our Quantum Edge
- Advancing Biotechnology: Drugs and Devices
- Advancing Biotechnology: Precision and Prediction

- Accelerating Our Energy Transition
- Strengthening Our Critical Minerals Supply Chain
- Regaining Leadership in Semiconductor Manufacturing
- Growing the Future of Materials Manufacturing





Tech Hub Highlights: Safe Autonomous Systems

Headwaters Hub (*Montana*): led by Accelerate Montana, aims to become a global leader in **smart**, **autonomous**, **photonic remote sensing technologies** with **\$41 million** in Tech Hubs awards serving Montana.

Headwaters hub integrates remote sensing systems with advances in embedded processors that **have built-in Al and machine learning (ML) capabilities** to develop and deploy smart photonic sensing systems coupled with autonomous systems to address critical defense, resource management, and disaster prevention needs.







Tech Hub Highlights: Safe Autonomous Systems

Ocean Tech Hub (*Massachusetts, Rhode Island*): led by the Rhode Island Commerce Corporation, seeks to develop, test, and commercialize emerging maritime artificial intelligence / machine learning-enabled robotics and sensors.

This Tech Hub is building emerging maritime AI-/ML-enabled robotics and sensors while leveraging its unique coastal assets—including seven commercial ports and shallow and deep ocean access—to establish manufacturing environments for rapid prototype testing and technology delivery to meet growing commercial demand.





Tech Hub Highlights: Safe Autonomous Systems

Tulsa Hub for Equitable and Trustworthy Autonomy (THETA) (*Oklahoma*): Led by Tulsa Innovation Labs, THETA aims to become a global leader in **developing and commercializing autonomous systems** for use cases ranging from agriculture and pipeline inspections to regional transportation with \$51 million in Tech Hubs awards.

THETA emphasizes the development of unmanned aircraft systems (UAS) and counter-UAS (CUAS), AI, and cybersecurity technologies to allow society to realize the maximum benefit of complex autonomous systems without compromising safety, security, privacy, or public trust.





Advanced Pharmaceutical Manufacturing (APM) Tech Hub (*Virginia*): Led by the Commonwealth Center for Advanced Manufacturing, APM seeks to accelerate the growth, innovation, and sustainability of the **U.S.-based advanced pharmaceutical** manufacturing industry to re-shore safe and affordable medicines via innovative hybrid and continuous flow manufacturing technologies.

This includes accelerating active pharmaceutical ingredient manufacturing processes by leveraging Al-/ML-based systems.







PRBio Tech Hub (*Puerto Rico*): Led by the Puerto Rico Science, Technology and Research Trust, PRBio aims to advance the region as a global leader in biotechnology through fast-tracking the discovery, development, manufacturing, and supply of next generation biotechnology and medical device products to detect, treat, and cure diseases and ailments.

PRBio enabling digital capabilities—e.g., **Al/ML**, **robotics**, **3D printing**, **and advanced 4.0 factory manufacturing**—to fast-track the discovery, development, manufacturing, and supply of next generation and disruptive products that detect, treat, and cure diseases and ailments.





Birmingham Biotechnology Hub (*Alabama*): The Birmingham Biotechnology Hub, led by Southern Research Institute, aims to become a global leader in **drug**, **vaccine**, **and diagnostics development** by applying artificial intelligence (AI)-driven biotechnology to increasing diverse representation in clinical genomic data and clinical trials.

Al and representative data is used to develop drugs, vaccines, and diagnostics that address the unique needs of underrepresented patient segments, improve diagnostic accuracy and drug efficacy, reduce timelines to develop new drugs and vaccines, enable rapid response to emerging health threats, and improve health outcomes of diverse patients at home and abroad.





Greater Philadelphia Region Precision Medicine Tech Hub (Pennsylvania, Delaware, Maryland, New Jersey): Led by the Ben Franklin Technology Partners of Southeastern Pennsylvania, aims to become a global leader in end-to-end precision medicine weaving together disparate technology applications—biotechnology, medical technology, genomics, synthetic biology supported by Al/ML, robotics, and more—to deliver new ways to diagnose, prevent, and treat disease, increasing evidence-based technology applications that improve morbidity and mortality and decrease health disparities.







Greater Philadelphia Region Precision Medicine Tech Hub (Pennsylvania, Delaware, Maryland, New Jersey): Led by the Ben Franklin Technology Partners of Southeastern Pennsylvania, aims to become a global leader in end-to-end precision medicine weaving together disparate technology applications—biotechnology, medical technology, genomics, synthetic biology supported by Al/ML, robotics, and more—to deliver new ways to diagnose, prevent, and treat disease, increasing evidence-based technology applications that improve morbidity and mortality and decrease health disparities.





Minnesota MedTech Hub 3.0 (Minnesota, Wisconsin): Led by the Minneapolis Saint Paul Economic Development Partnership, aims to position Minnesota as a global center for "Smart MedTech" by integrating artificial intelligence (AI), machine learning, and data science into medical technology, allowing for regional information-sharing and innovative collaboration.







Wisconsin Biohealth Tech Hubs (Wisconsin): Led by BioForward Wisconsin, aims to position Wisconsin as a global leader in personalized medicine, an emerging healthcare approach that tailors tests, treatments, and therapies informed by a patient's unique genetic code, medical record, and environment to guide decisions about tests, treatments, and therapies tailored for them with AI/ML techniques. Wisconsin Biohealth has recieved \$49 million in Tech Hubs awards to serve Wisconsin.







Tech Hub Highlights: Energy Transition

Gulf Louisiana Offshore Wind Propeller (Louisiana): Led by Louisiana State University, aims to transition Louisiana's energy economy from its legacy of oil and gas to **offshore wind and renewable energy**.

This Tech Hub connects Al into the Hub's energy infrastructure, port and shipbuilding network, and local workforce to establish a domestic offshore wind supply chain and expand harvestable offshore wind sites.





Tech Hub Highlights: Materials Manufacturing

American Aerospace Materials Manufacturing Tech Hub (Washington, Idaho): Led by American Aerospace Materials Manufacturing Center, aims to develop new domestic supply chains to meet the immediate demand for high-rate production of advanced composite aerostructures in defense and commercial markets. This work incorporates automation, robotics, Al, and sophisticated tooling into aerospace workforce training.





Additional Resources

EDA also supports resources and programs to help regions execute, build and more easily connect with each other to learn, test and pursue entrepreneurial and innovative approaches to sustainable economic growth and prosperity.

- Tools and Resources for Economic Developers
 - National Economic Research and Resilience Center (Argonne National Labs)
 - Data dashboards for economic resilience, economic development capacity, program eligibility
 - Inclusive Recovery Tool Kit (New Growth Innovation Network)
- New Investments in America's Economic Development Infrastructure
 - <u>Economic Recovery Corps</u>
 - <u>Communities of Practice</u>
 - TBED, EDDs, RLFs, Indigenous, Coal, Manufacturing Communities and more.



Questions & Contact Info

Tech Hubs Program Office

techhubs@eda.gov

Tech Hubs Online

techhubs.gov







Questions & Answers

Key Dates



Milestone	Date
NOFO Published	July 22, 2024
Informational Webinar	July 25, 2024
Proposers Day	August 20, 2024 (today)
Concept Papers due	September 30, 2024
Proposal Invitation	November 2024
Full Proposal Due	January 2025 (deadline will be specified in the invitation to submit Full Proposals)
Selection Announcement & Anticipated Award	Spring 2025

Questions



Answers to Frequently Asked Questions can be found on the OAM website:

https://www.nist.gov/oam/ai-resilient-manufacturing-institute-competition



ManufacturingUSA@nist.gov Subject line: "Al for Resilient Manufacturing"



Informal Teaming Discussions





What to Expect



Purpose: To provide a networking opportunity to support the formation of effective proposal teams

- Participants can build off of the earlier "Teaming for a Great Proposal" session
- Suggested topics are based on earlier discussions
- Federal employees are excluded from teaming conversations

Suggested Process



- > Each table will be given a suggested topic for discussion.
- Attendees are welcome to stay at their table or move around.
- Please be sure to introduce yourselves.
- Space is also available in the bistro area outside the main room and on the adjoining patio.
- > Event will end promptly at 5:00 pm.

Suggested Table Topics



RED	AI Engineering Skills
PINK	Manufacturing Processing Engineering Skills
ORANGE	Supply Chain
YELLOW	AI Safety and Security/Risk Management/Regulatory Expertise
BLACK	Hardware & Equipment
GREEN	Education/Workforce Convening Skills
DARK BLUE	Relationship Development
LIGHT BLUE	Strategic Thinking and Data Infrastructure
PURPLE	Business Management Skills
WHITE	Teaming and Human Computer Interactions
* STAR *	Primary Applicants



Participant List

Teaming List



