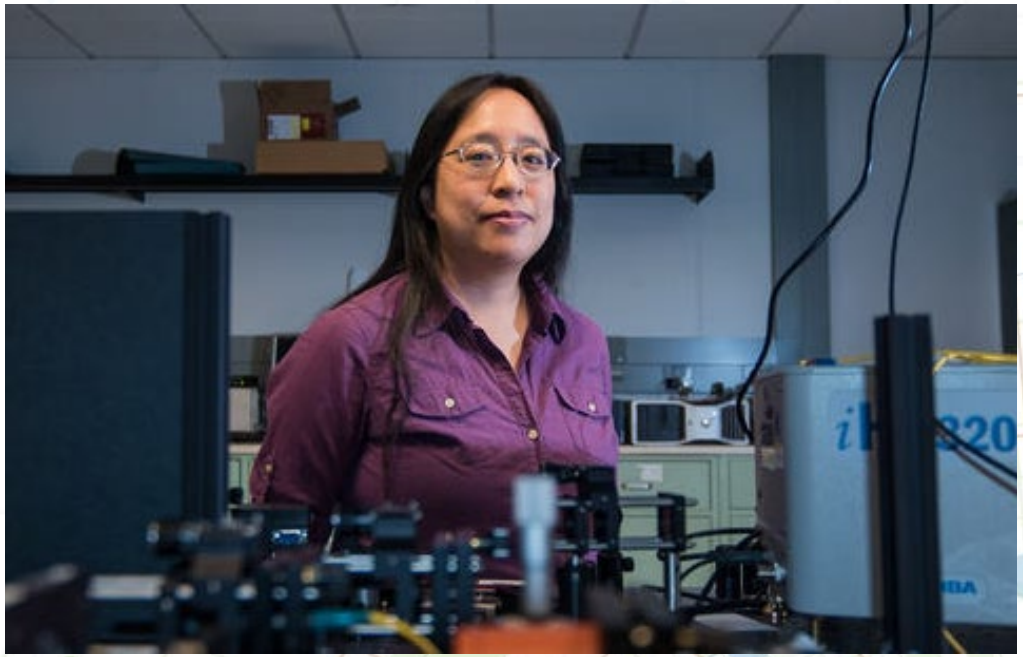
NIST ITL Lab Updates
Jim St.Pierre

July 12, 2023

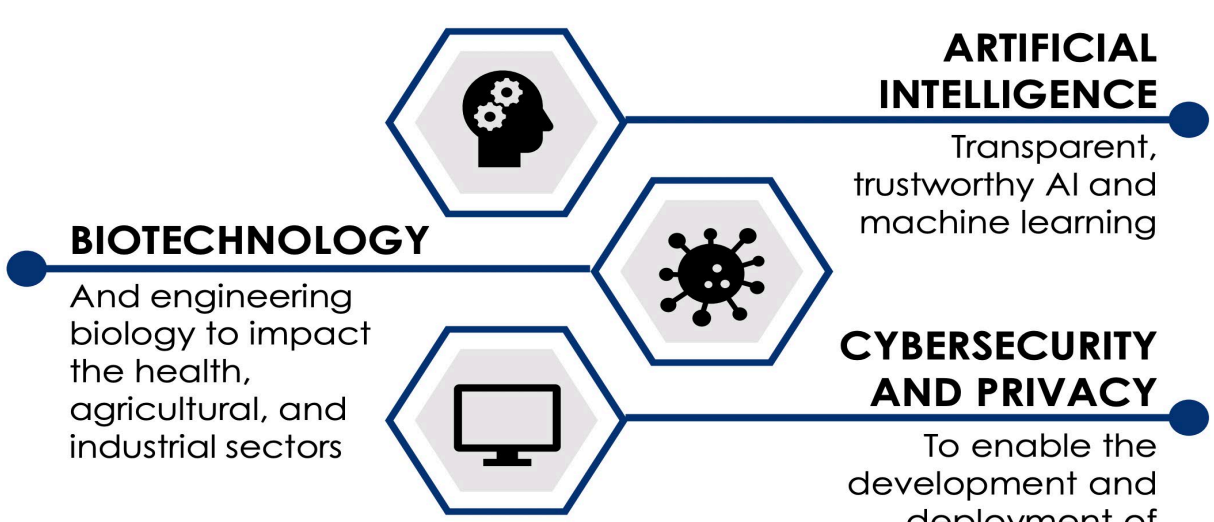
National Institute of Standards and Technology
U.S. Department of Commerce

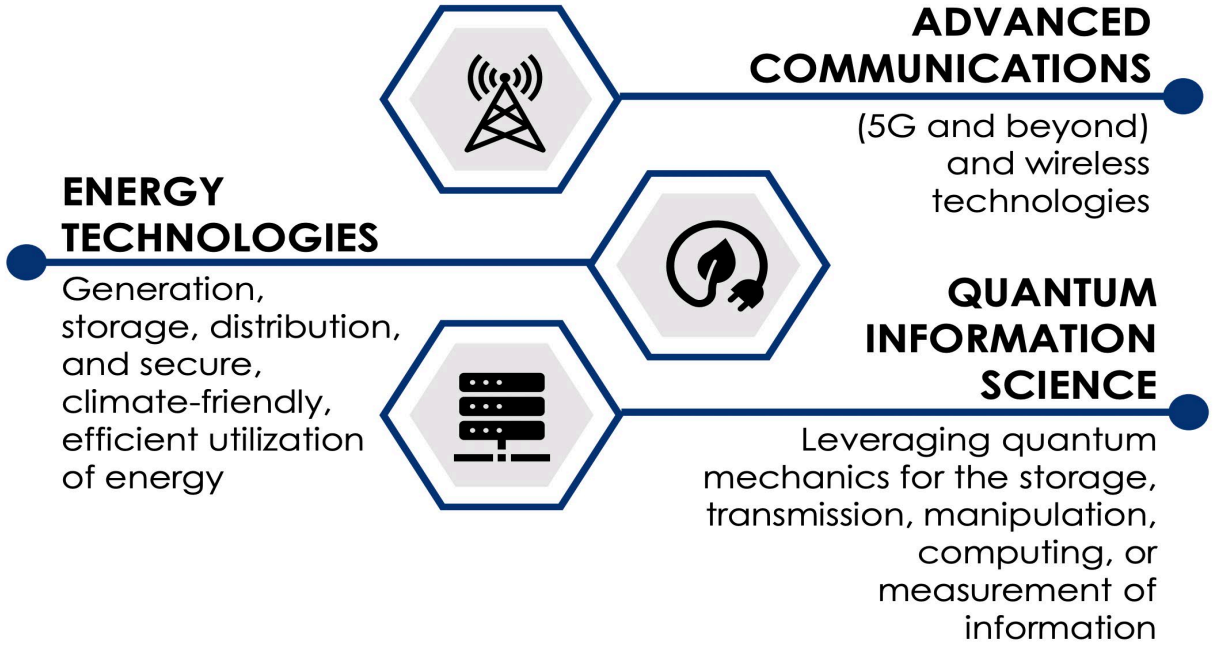
Cultivating Trust in IT and Metrology



National Institute of Standards and Technology
U.S. Department of Commerce

NIST Wide Critical and Emerging Technologies





ITL Mission Areas

Maximize the benefits of information technology (IT) to society through a balanced IT measurement science and standards portfolio of three major activities:

1) fundamental research in mathematics, statistics, and IT;
2) 2) applied IT research and development; and
3) 3) standards development and technology transfer.

ITL has identified five priority areas through which ITL research will maximize the benefits of IT and metrology to society:

1) cybersecurity,
2) the Internet of Things,
3) artificial intelligence,
4) reliable computing, and
5) future computing technologies.

NIST AI PROGRAM

CONDUCT FOUNDATIONAL RESEARCH TO ADVANCE TRUSTWORTHY AI TECHNOLOGIES	ADVANCE AI RESEARCH AND INNOVATION ACROSS THE NIST LABORATORY PROGRAMS	ESTABLISH BENCHMARKS AND DEVELOP METRICS TO EVALUATE AI TECHNOLOGIES
PARTICIPATE AND LEAD IN THE DEVELOPMENT OF STANDARDS TO ADVANCE AI INNOVATION	COCONTRIBUTE NIST'S TECHNICAL EXPERTISE TO DISCUSSIONS AND DEVELOPMENT OF POLICIES	ENSURE THAT NIST HAS RESOURCES AND EXPERTISE TO CARRY OUT ITS AI PROGRAMS

TRUSTWORTHY AND RESPONSIBLE AI @ NIST

Cultivate trust in the design, development, use and governance of artificial intelligence technologies and systems.

Guidance and Tools

AI Risk Management Framework, AI Standards

Research and Development

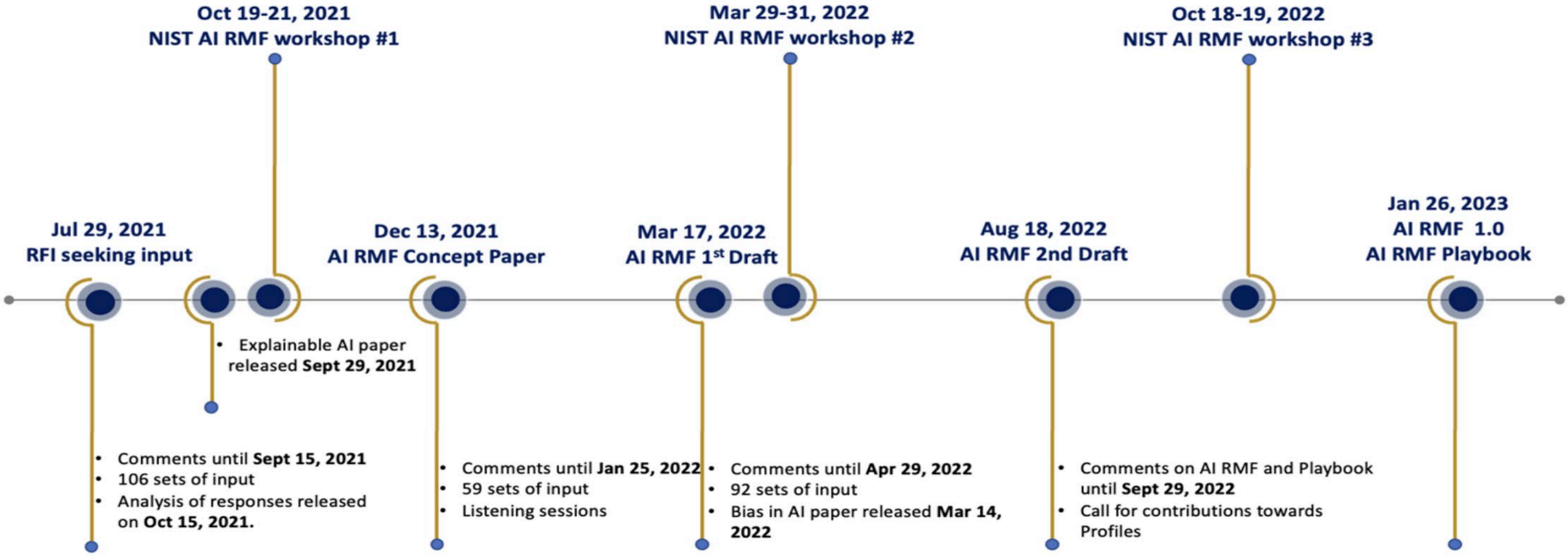
National AI Institute on Trustworthy AI (TRAILS)

Lead and Convene

National AI Advisory Committee, international engagements, and more.

NIST AI RMF

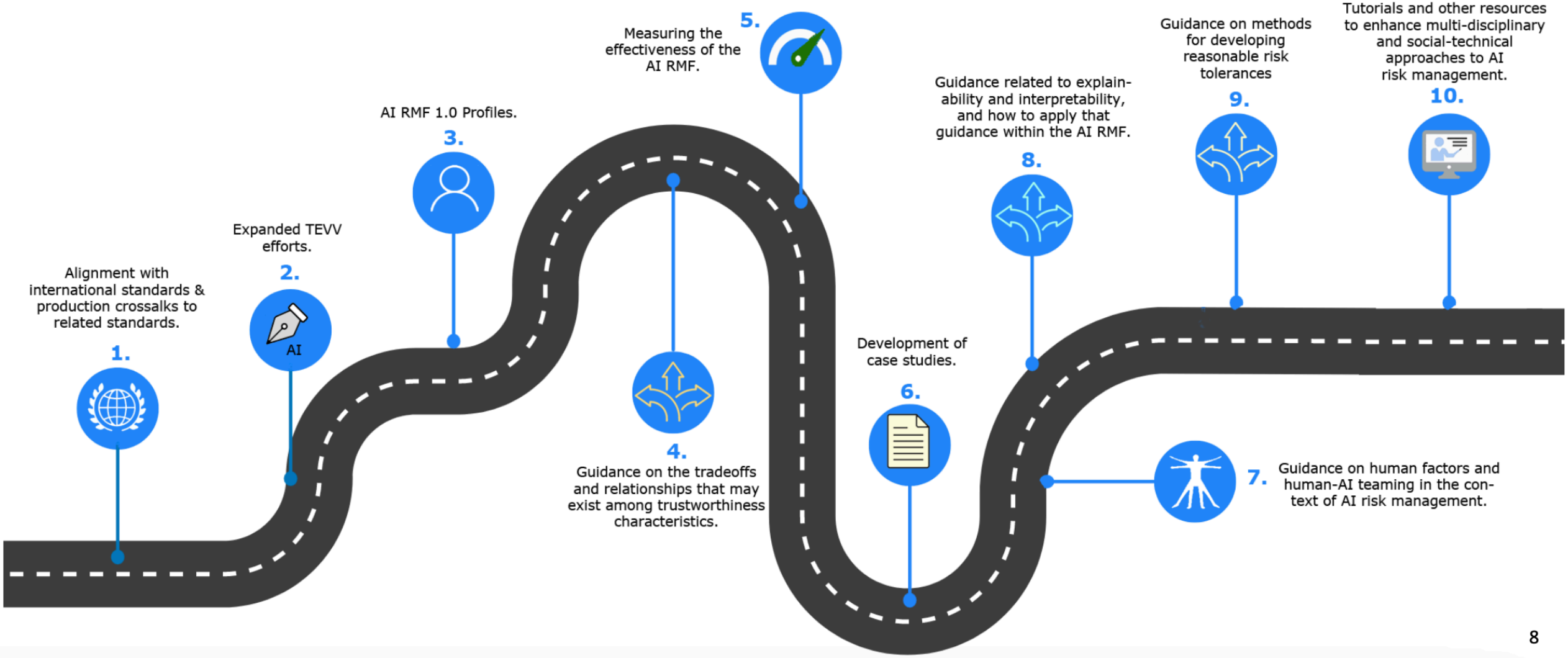
A voluntary resource for organizations designing, developing, deploying, or using AI systems to manage AI risks and promote trustworthy and responsible AI



AI RMF CORE

Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact

AI RMF ROADMAP

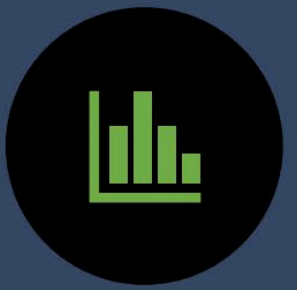


NIST TRUSTWORTHY AI RESOURCE CENTER

AI RMF PLAYBOOK

AI RMF PROFILES

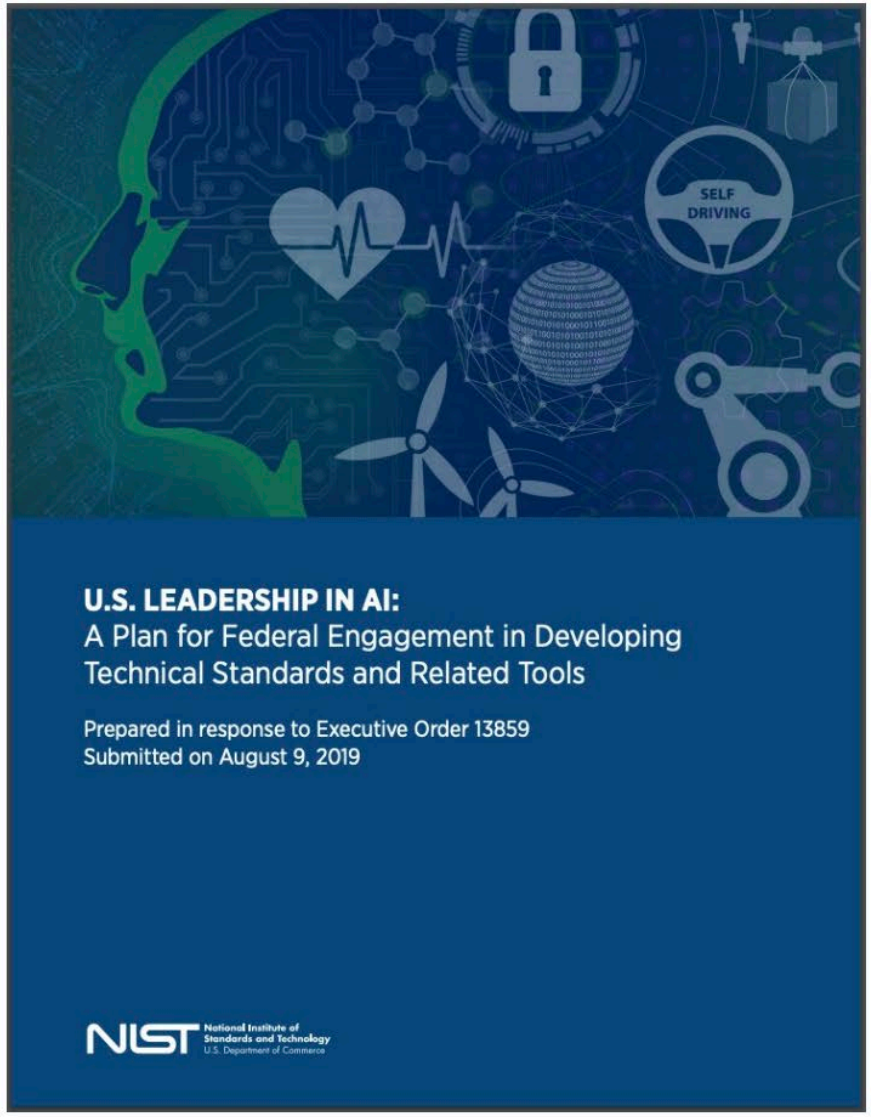
AI RISK GLOSSARY



AI METRICS HUB

...AND MORE
airc.nist.gov

USG STANDARDS AI COORDINATOR



Outreach to connect with all known federal efforts relating to AI standards development and use.

Support and contribute to development of AI standards. Develop crosswalk to international standards.

TRUSTWORTHY AI IN LAW AND SOCIETY (TRAILS)

"Today, the ability to measure AI system trustworthiness and its impacts on individuals, communities and society is limited. TRAILS can help advance our understanding of the foundations of trustworthy AI, ethical and societal considerations of AI, and how to build systems that are trusted by the people who use and are affected by them." Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio

Led by UNIVERSITY OF MARYLAND

In partnership with THE GEORGE WASHINGTON UNIVERSITY WASHINGTON, DC, MORGAN STATE UNIVERSITY, CORNELL UNIVERSITY FOUNDED A.D. 1865

Co-Funded by NSF, NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

INTERNATIONAL ENGAGEMENT

EXAMPLES;

US-UK COOPERATION ON AI R&D

OECD.AI Policy Observatory

OECD NETWORK OF EXPERTS ON AI

TRADE AND TECHNOLOGY COUNCIL TECHNOLOGY (STANDARDS, AI)

QUADRILATERAL SECURITY DIALOGUE STANDARDS SUB-GROUP

NCCOE Activities

Center Partnerships with State and County Renewed

The Department of Commerce's National Institute of Standards and Technology (NIST), the state of Maryland and Montgomery County, Maryland, have renewed their partnership in support of the National Cybersecurity Center of Excellence (NCCoE), a collaborative hub where industry, government and academic experts work together to solve pressing cybersecurity challenges.

NCCOE Projects Underway

[5 Step Strategy for Enterprise Mobile Deployment]

[NCCoE Seeks Collaborators for New Water/Wastewater Sector Project]

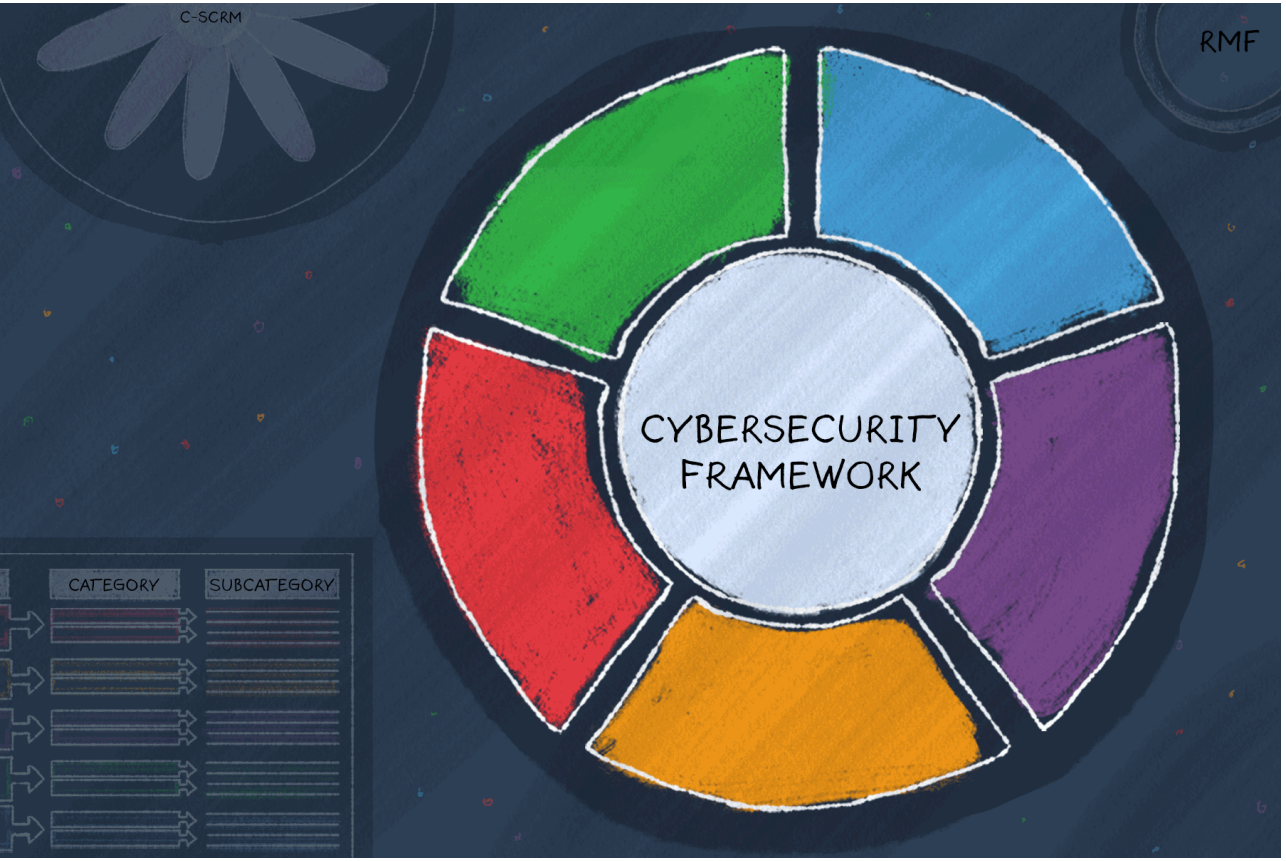
[NCCoE Releases Draft Cybersecurity Framework Profile for Genomic Data]

[Open for Public Comment: Draft NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks]

[NCCoE IoT Onboarding Team Releases New Practice Guidance (Preliminary Draft NIST SP 1800-36, Vols. B–E)]

[NCCoE Releases Preliminary Draft NIST SP 1800-38A, Migration to Post Quantum Cryptography for Public Comment]

Revision to Cybersecurity Framework



Discussion Draft of the NIST CSF 2.0 Core - feedback on this discussion draft may be submitted at any time. Comments to inform the upcoming complete NIST CSF 2.0 were submitted by May 31st.

Encryption Updates:

The END OF DES. Disallowed after December 31, 2023

Light Weight Selection; 6th WS Held on June 21.

AES Modes WS Planned for Oct

PQC Draft Standards “Soon”

ITL Quantum Information (QI) Program

Goals: *Understand potential & threats of QI for IT. Develop metrology for quantum-based IT.*

Joint Center for Quantum Information and CS (QuICS)

- Developed Error Correction Zoo, an online catalog of ~430 quantum and classical error-correction codes.
- Settled long-standing conjecture about whether all quantum algorithms can be implemented by intervening low-depth quantum circuits and polynomial-time classical computation (presented at STOC).
- Developed AI-based methods for tuning quantum dots for use as qubits.

Quantum Characterization

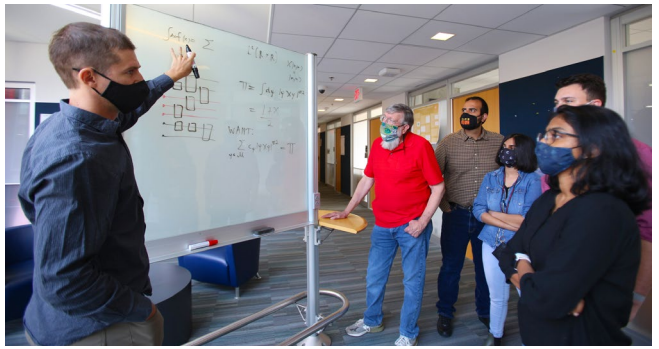
- Developed improved methods for quantum state and process tomography.
- With PML, demonstrated entanglement of macroscopic vibrating drumheads *Physics World's* top breakthrough of 2021. Published in *Science*.

Quantum Networking

- Major participant in the DC-QNet, a regional testbed, with ARL, NRL, USNO, NASA, and NSA.
- Synchronized network nodes to below 200 ps over 128 km, distributed entanglement over 130 km.

Quantum Information Applications

- Developed most data-efficient protocols for generating random numbers from loophole-free Bell tests.
- Leading community-based process for standardizing public-key cryptosystems for the post-quantum era.



NIST National Vulnerability Database (NVD)

- New APIs for Industry Integration and Use
- The NVD added information to its CVE detail pages to identify vulnerabilities appearing in CISA's Known Exploited Vulnerabilities (KEVS) Catalog.
- New Data linking to SWIDS and NSRL

CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	20030
HIGH	54235
MEDIUM	52315
LOW	2277

CVE Status Count

Total	219488
Awaiting Analysis	309
Undergoing Analysis	231
Modified	73387
Deferred	115
Rejected	12778

NVD Contains

CVE Vulnerabilities	219488
Checklists	614
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	10286
CPE Names	1105523

NICE

CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT FUNDING OPPORTUNITY

NICE announced a new Notice of Funding Opportunity (NOFO) from the National Institute of Standards and Technology (NIST).

NIST is offering funding to establish Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development. RAMPS will support the NIST-led NICE program.

NEW DEADLINE: JULY 28, 2023 | NICE K12 Conference Call for Proposals

Conference Dec 2023 in AZ

JUST PUBLISHED: NICE FRAMEWORK COMPETENCY AREAS, NISTIR 8355

Some Recognitions

NIST SW Testing paper from 2013 that introduced the SW Combinatorial Test Tool has been recognized at the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Software Testing, Verification and Validation (ICST). It's the most influential paper in the "practical" category published during the past 10 years.

Rodney Petersen Receives the National Centers of Academic Excellence in Cybersecurity 2023 Service Recognition Award

Karen Wetzel Receives the National Centers of Academic Excellence in Cybersecurity 2023 Service Recognition Award

DOC Silver Medal Award: The group is recognized for its exceptional leadership and outstanding technical innovation to strengthen the resilience of the nation's Positioning, Navigation, and Timing (PNT) infrastructure and services.

QUESTIONS?