Cultivating Trust in IT and Metrology

NIST Information Technology Laboratory Update
Kevin Stine
Director, ITL

March 20, 2024

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

ITL Updates

Rodney Petersen
Interim Chief
Applied Cybersecurity Division

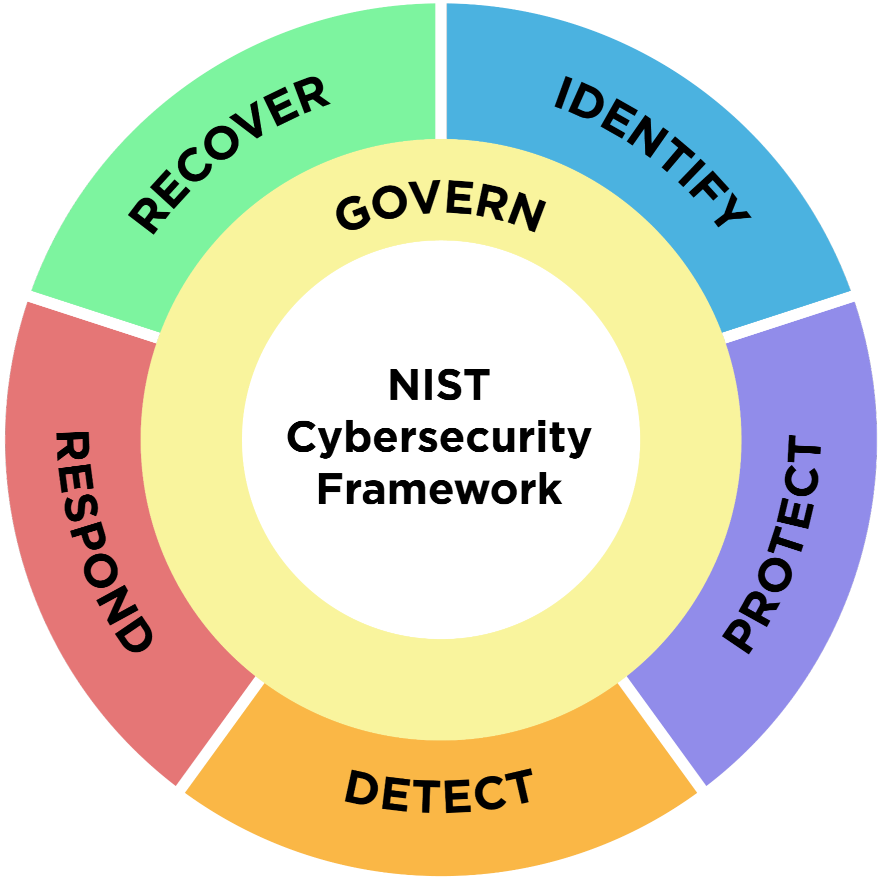
Kamie Roberts
AI Executive Order Program
Manager

Select Program Updates

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

Cybersecurity Framework 2.0

- NIST has updated the widely used Cybersecurity Framework (CSF)—its landmark guidance document for **managing cybersecurity risk**.
- Organized by Six Functions — **Govern, Identify, Protect, Detect, Respond,** and **Recover.**
- Together, they provide a comprehensive view for understanding, communicating, and managing cybersecurity risk.



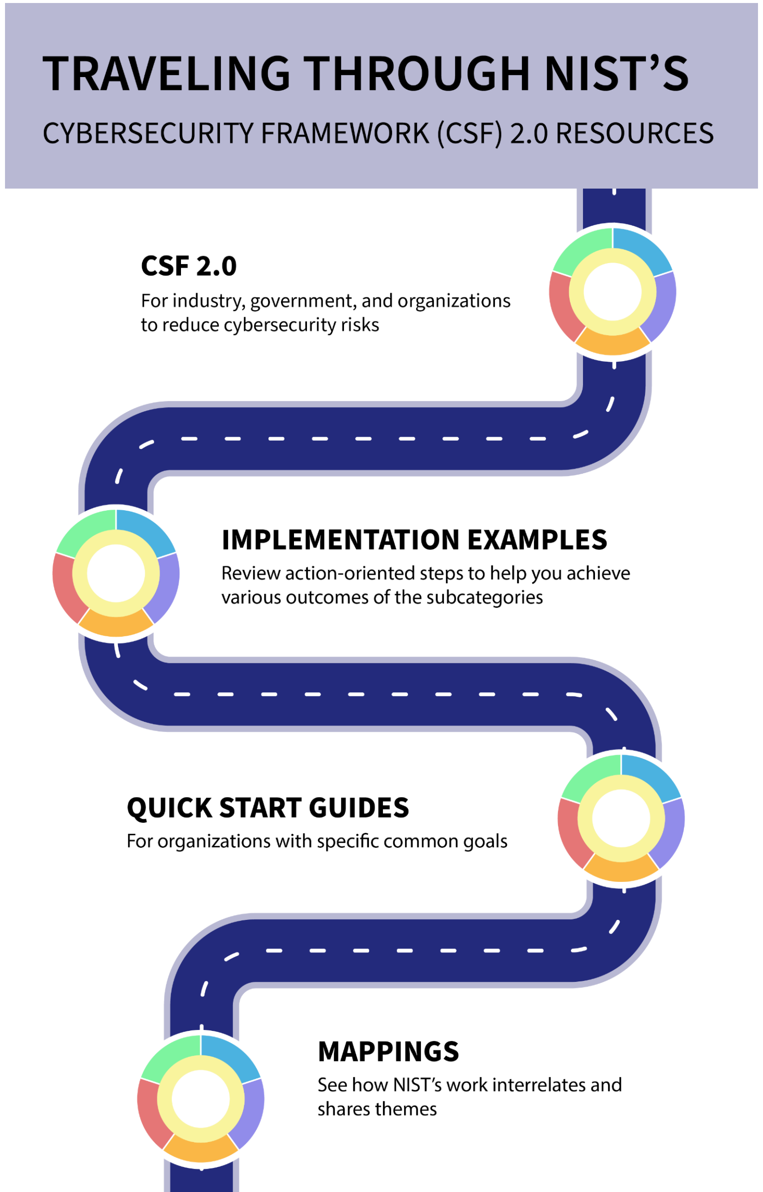
CSF 2.0 | What Makes it Different?

- CSF 2.0 can help **all organizations** – not just those in critical infrastructure – manage and reduce risks.

- It improves on prior versions; we listened to your feedback, made key updates, **developed new resources and tools**, and adjusted our guidance based on today's cybersecurity environment.

- NIST's suite of resources offers **practical and actionable suggestions** to help organizations immediately improve their cybersecurity posture (focus on *how* the CSF can be implemented).

- The CSF 2.0 is about a **suite of resources** that aims to help **all organizations** – not just those in critical infrastructure – manage and reduce risks.



TRAVELING THROUGH NIST'S

CYBERSECURITY FRAMEWORK (CSF) 2.0 RESOURCES

CSF 2.0

For industry, government, and organizations to reduce cybersecurity risks

IMPLEMENTATION EXAMPLES

Review action-oriented steps to help you achieve various outcomes of the subcategories

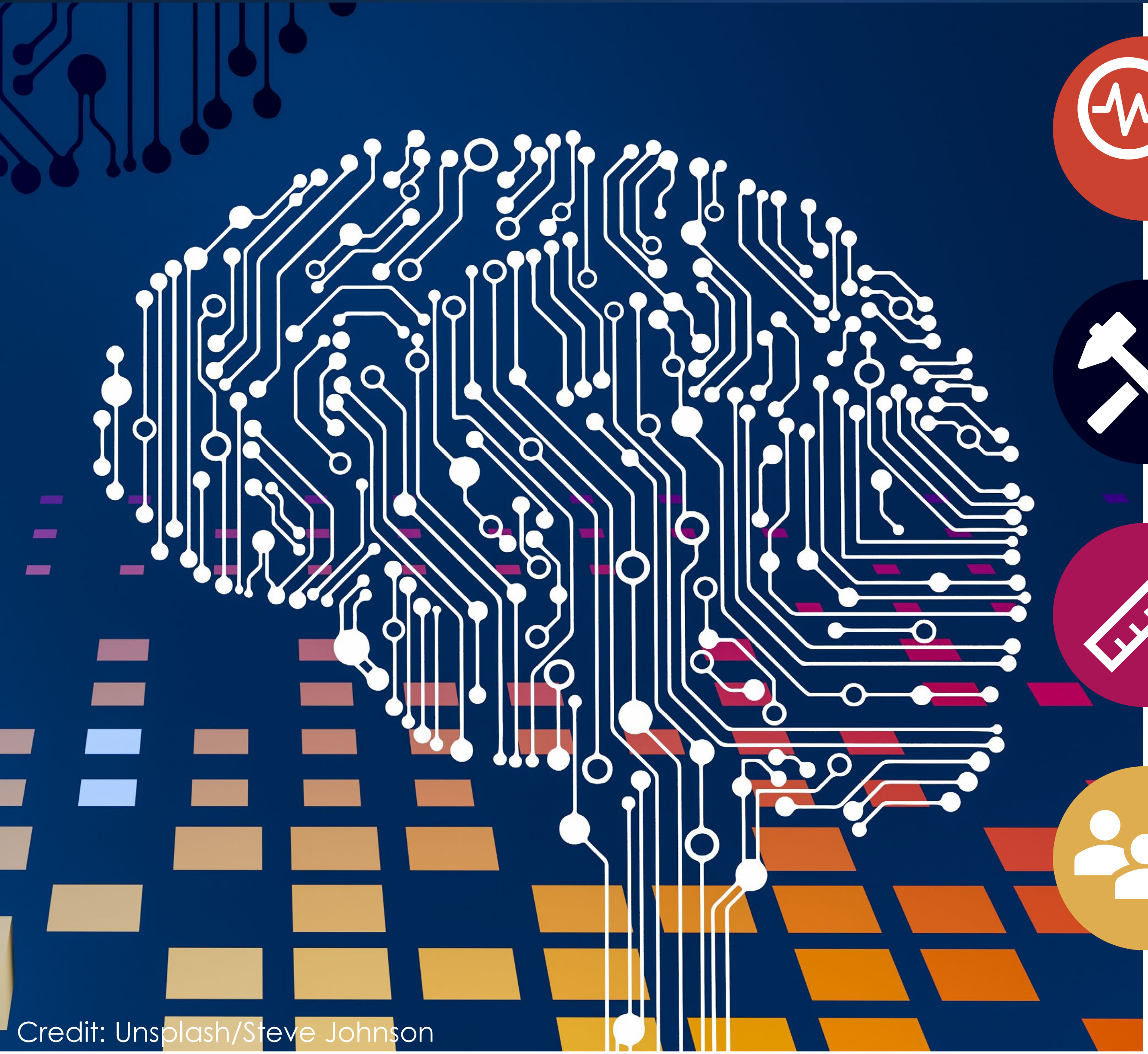
QUICK START GUIDES

For organizations with specific common goals

MAPPINGS

See how NIST's work interrelates and shares themes

Artificial Intelligence



Credit: Unsplash/Steve Johnson

- Fundamental and Applied AI Research
- Guidance, Tools, and Frameworks
- Measurement, Evaluation, and Standards
- Lead and Convene Domestically and Internationally

Executive Order 14110

The President's Executive Order (E.O.) on Safe, Secure, and Trustworthy Artificial Intelligence (14110) directs NIST to:

Create Guidance

- Generative AI and dual-use foundation models
- Differential-privacy guarantee protections
- Red-teaming/testing
- Authenticity and provenance of synthetic content

Develop Evaluation & Testing

- Test environments for evaluating AI capabilities, including those that could cause harm
- Availability of testbeds supporting the development of safe, secure, and trustworthy AI technologies

Engage with Stakeholders & Develop Standards

- Global engagement on AI standards
- Synthetic nucleic acid synthesis providers engagement
- Minimum risk-management practices

NIST's Progress on E.O. Assignments

Credit: Gerd Altmann from Pixabay

- Request for Information (RFI) to inform NIST's assignments
- Draft Guidelines for Evaluating Differential Privacy
- Secure Software Development Framework Workshop
- Pre-release testing of NIST's Dioptra infrastructure

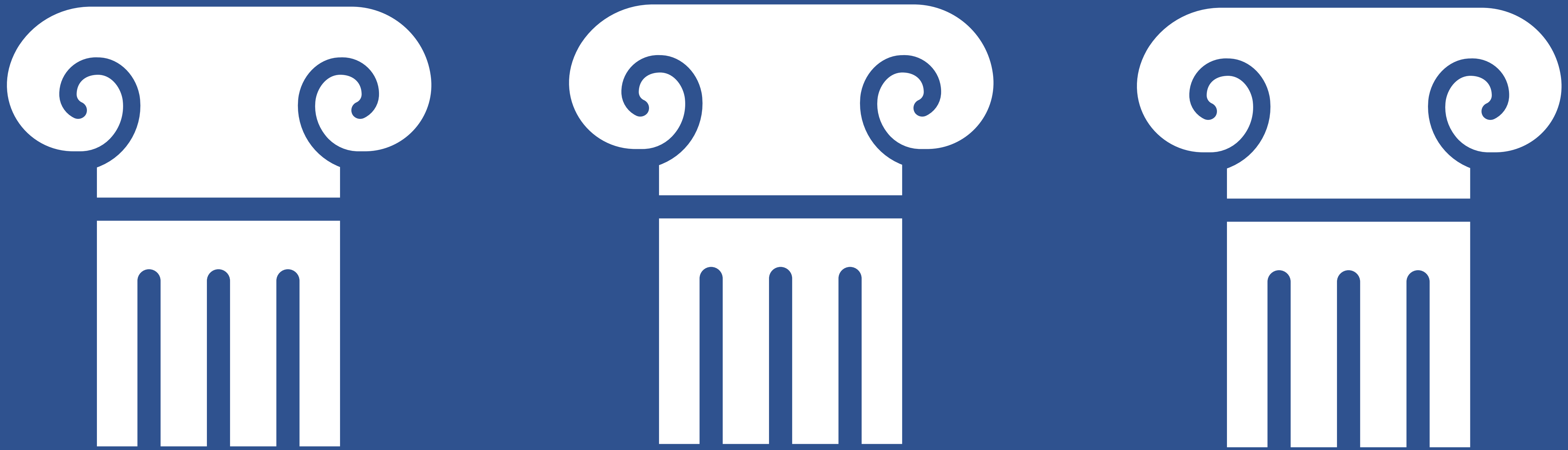
United States AI Safety Institute (USAISI)

The USAISI's primary mission is to build the science necessary for safe development and use of trustworthy AI.

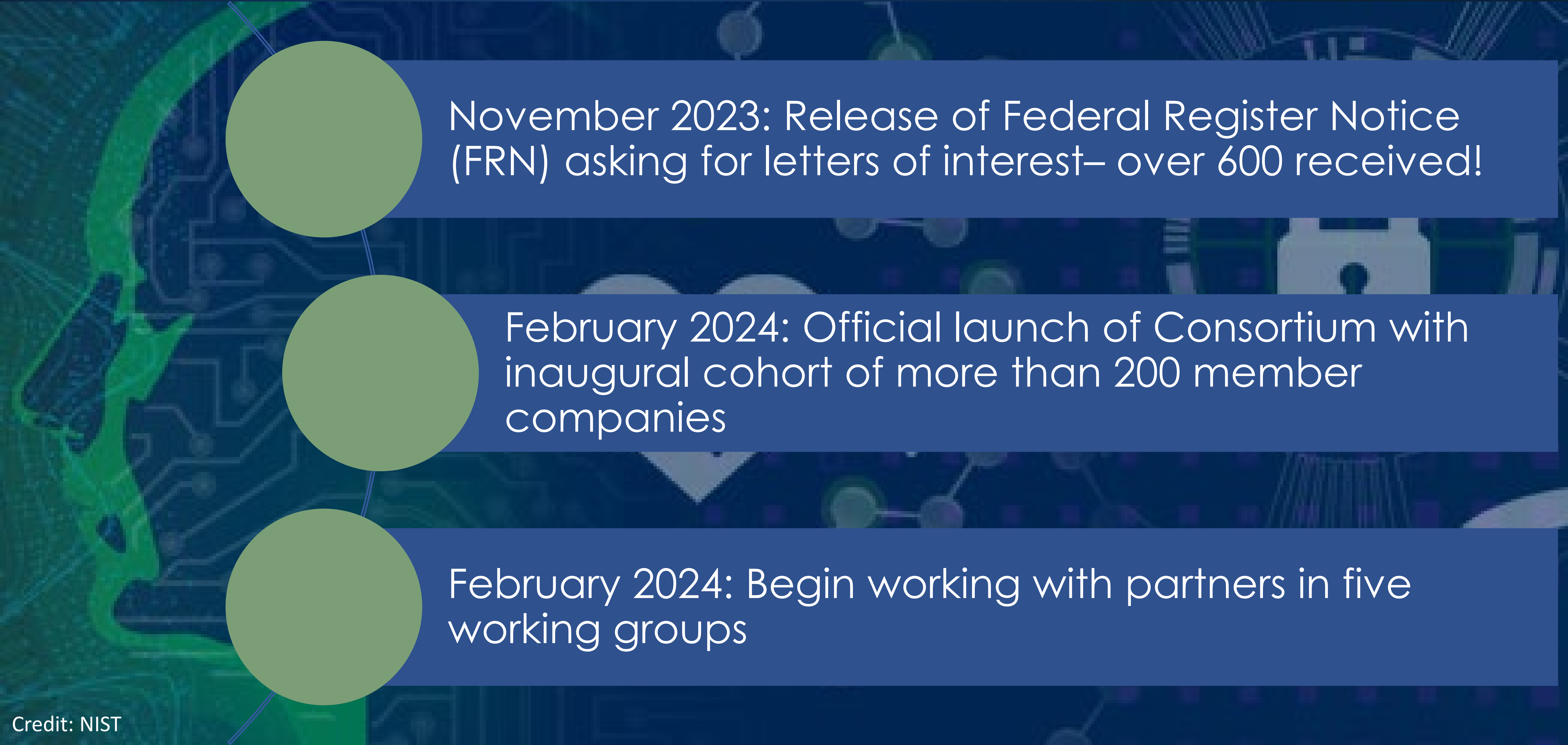
Research

Implementation

Engagement & Operations



USAISI Consortium



November 2023: Release of Federal Register Notice (FRN) asking for letters of interest– over 600 received!

February 2024: Official launch of Consortium with inaugural cohort of more than 200 member companies

February 2024: Begin working with partners in five working groups

Credit: NIST

AI: Adversarial Machine Learning Report

Adversarial Machine Learning Taxonomy and Terminology Report

- Identifies vulnerabilities of machine learning and AI
- Establishes common language for understanding threats and mitigation methods

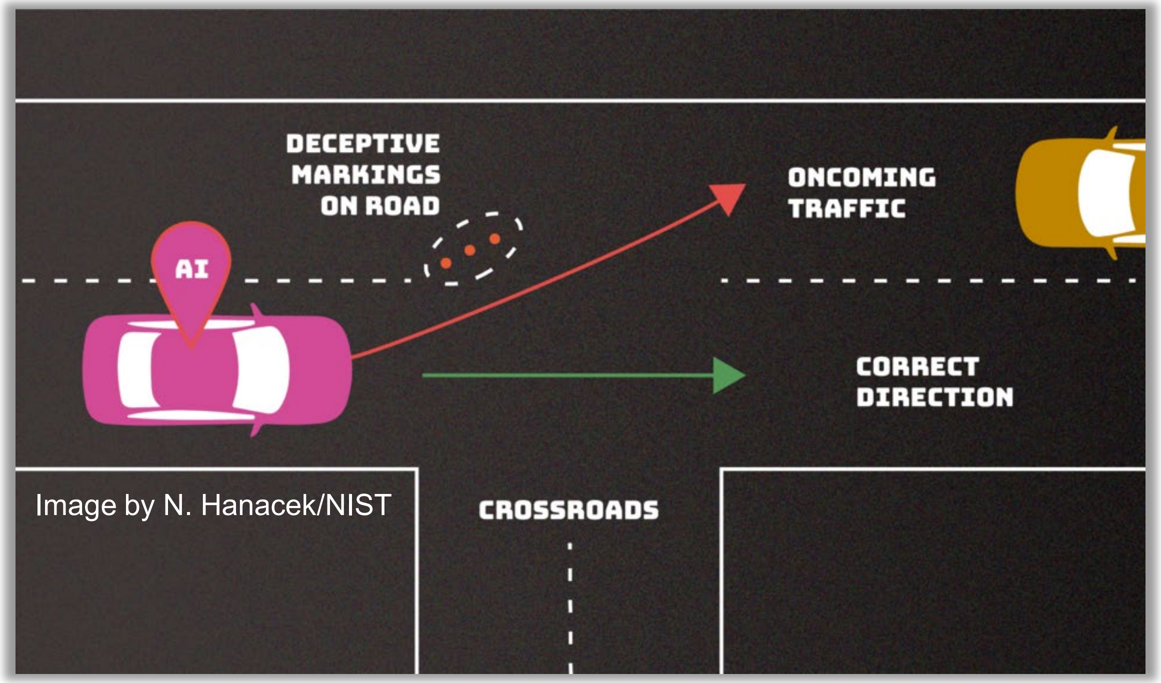


Image by N. Hanacek/NIST

AI: What's Next for NIST?

Credit: Gerd Altmann from Pixabay

AI E.O. Deliverables

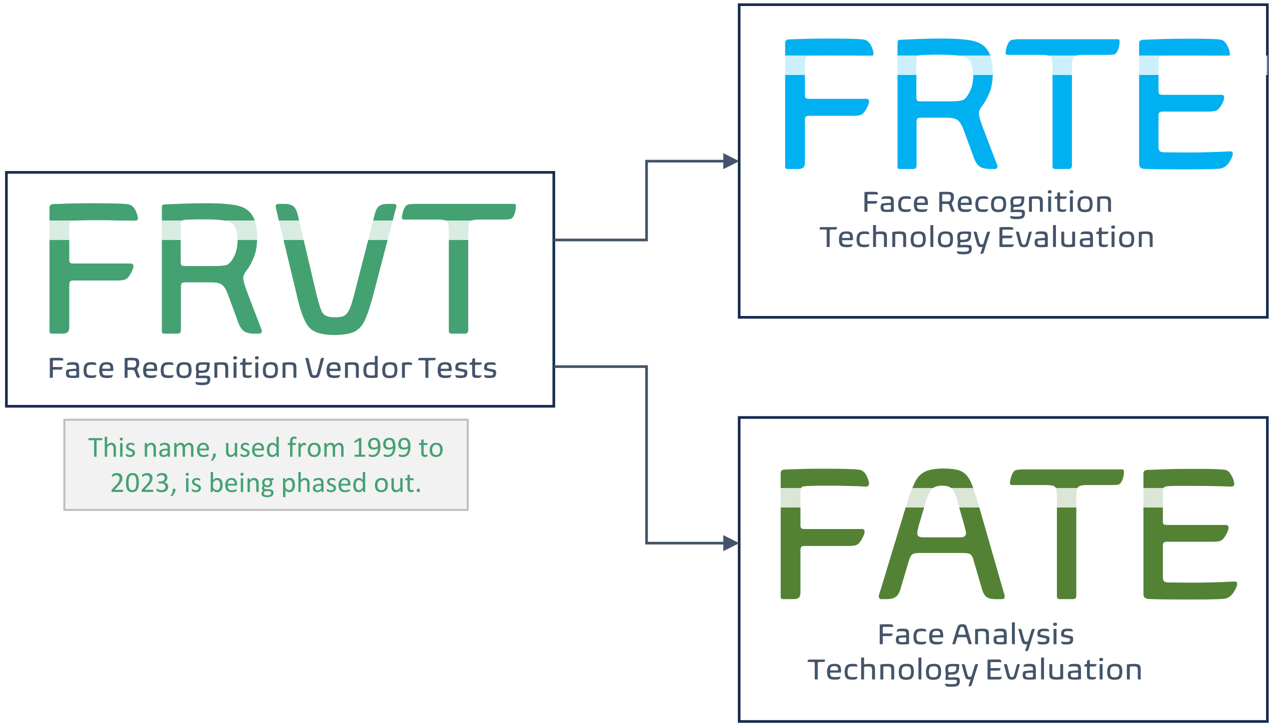
- Report on synthetic content
- Guidelines for red-teaming
- Generative AI companion resource
- Secure Software Development Framework companion resource
- Plan for global engagement on AI standards
- Pilot program for test evaluations

USAISI

- Develop Consortium work plans
- Nationwide workshops in support of working group activities

Face Recognition

FRVT Split :: Distinguishing recognition from analysis


FRVT

Face Recognition Vendor Tests

This name, used from 1999 to 2023, is being phased out.

FRTE

Face Recognition Technology Evaluation

FATE

Face Analysis Technology Evaluation

- 1:1 Verification
- 1:N Search
- Twins Disambiguation
- 1:N Face + Iris
- Face in Video Evaluation

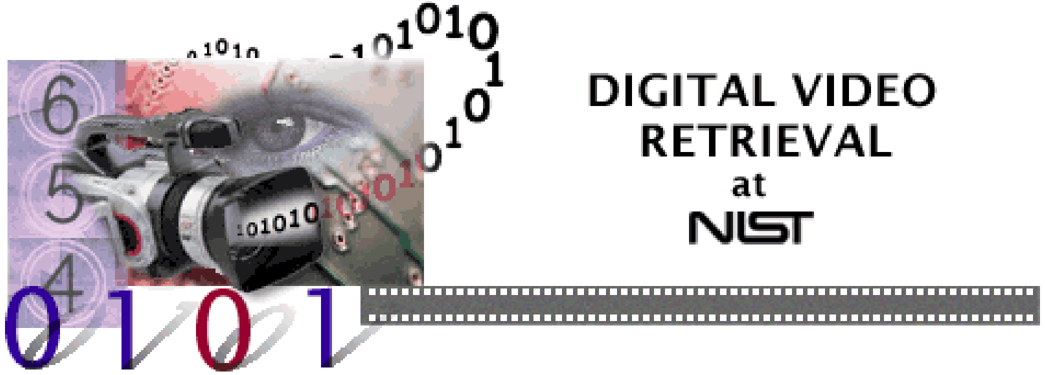
- Morph Detection
- Quality Summarization
- Quality Defect Detection
- Presentation Attack Detection
- Age Estimation

Benchmarks are: Independent + Free + Open globally + Regular + Repeatable + Fair + Black box IP-protecting + Large-scale + Statistically robust + Public + Transparent + Extensible

Information Retrieval

TREC workshop at NIST, Nov 18-22, 2024
- TREC, TRECVID, and TAC folded into a single venue
- LLMs make past distinctions between media and task less important
- So it’s best to have all the communities together.

New tracks for 2024 include:
- Retrieval Augmented Generation
- Biomedical Generative Retrieval
- Multilingual search and report generation
- Video-to-text
- Recognizing entities, events, and relations



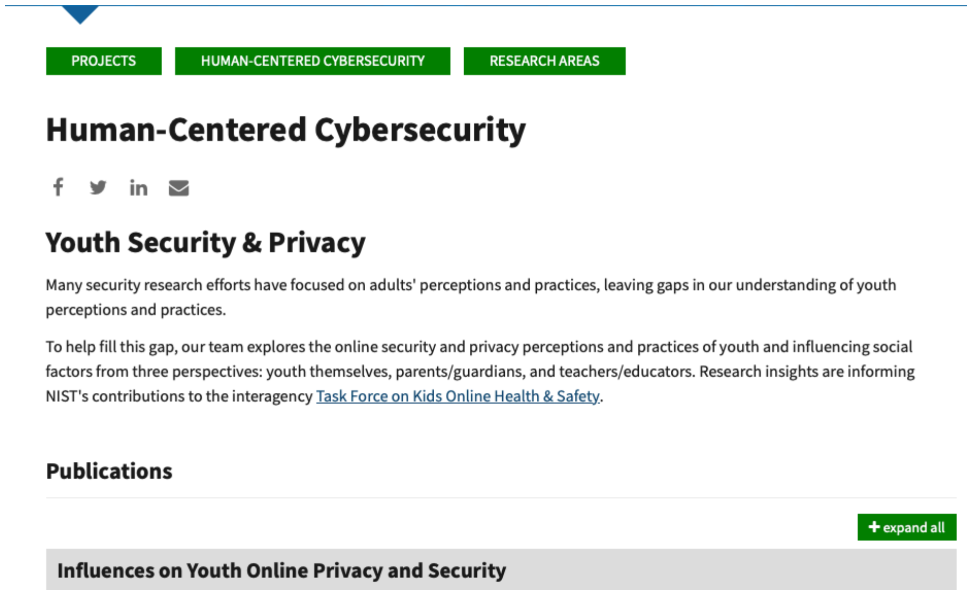
Youth Security & Privacy

- NIST Research on youth online cybersecurity and privacy practices
  - https://csrc.nist.gov/Projects/human-centered-cybersecurity/research-areas/youth-security

- Findings on how parents, guardians, and teachers influence online youth behavior are informing the White House Interagency Task Force on Kids Online Health and Safety (KOHS)
  - https://www.samhsa.gov/kids-online-health-safety-task-force

- NIST active in 3 KOHS working groups:
  - Best Practices for Parents, Caregivers and Youth
  - Status of Industry Effort and Technology
  - Research Agenda

- KOHS Guidance documents expected ~summer FY24



Human-Centered Cybersecurity

Youth Security & Privacy

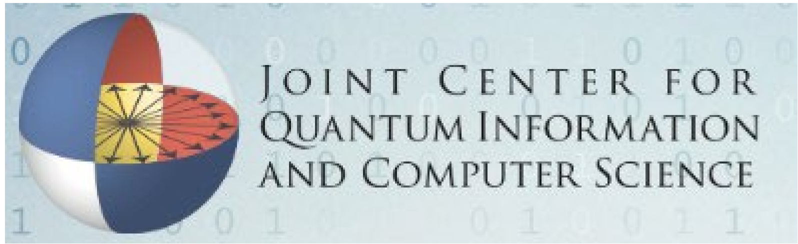
Many security research efforts have focused on adults' perceptions and practices, leaving gaps in our understanding of youth perceptions and practices.

To help fill this gap, our team explores the online security and privacy perceptions and practices of youth and influencing social factors from three perspectives: youth themselves, parents/guardians, and teachers/educators. Research insights are informing NIST's contributions to the interagency Task Force on Kids Online Health & Safety.

Publications

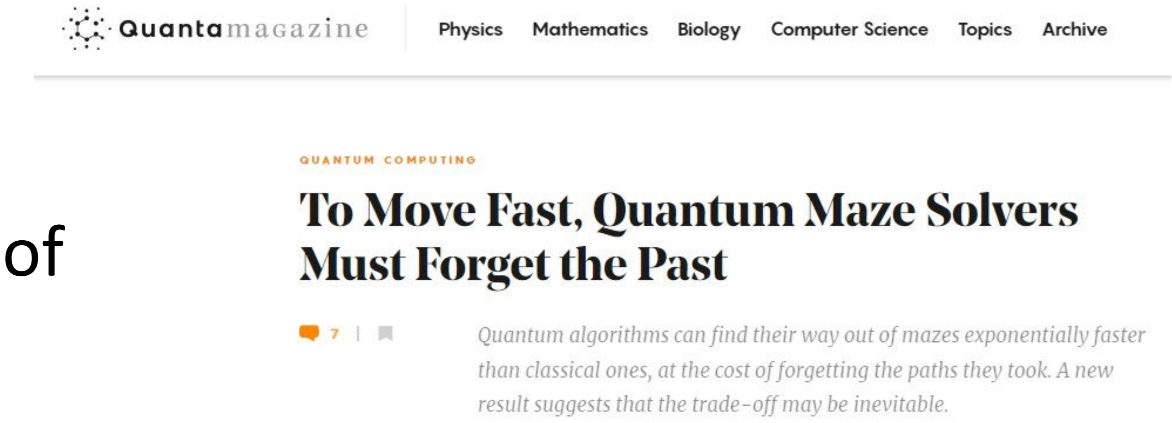
Influences on Youth Online Privacy and Security

NIST – ITL and Quantum Information



QuICS: Joint Center at UMD College Park

- 14 Fellows (8 NIST), 20 postdocs, 67 students
- Focus: quantum computer science
- 70 research papers issued in calendar 2023



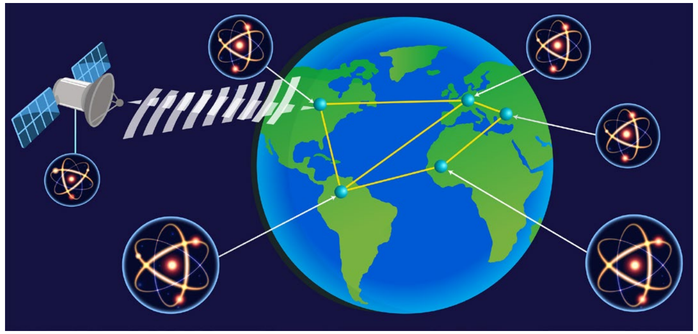
QUANTUM COMPUTING

To Move Fast, Quantum Maze Solvers Must Forget the Past

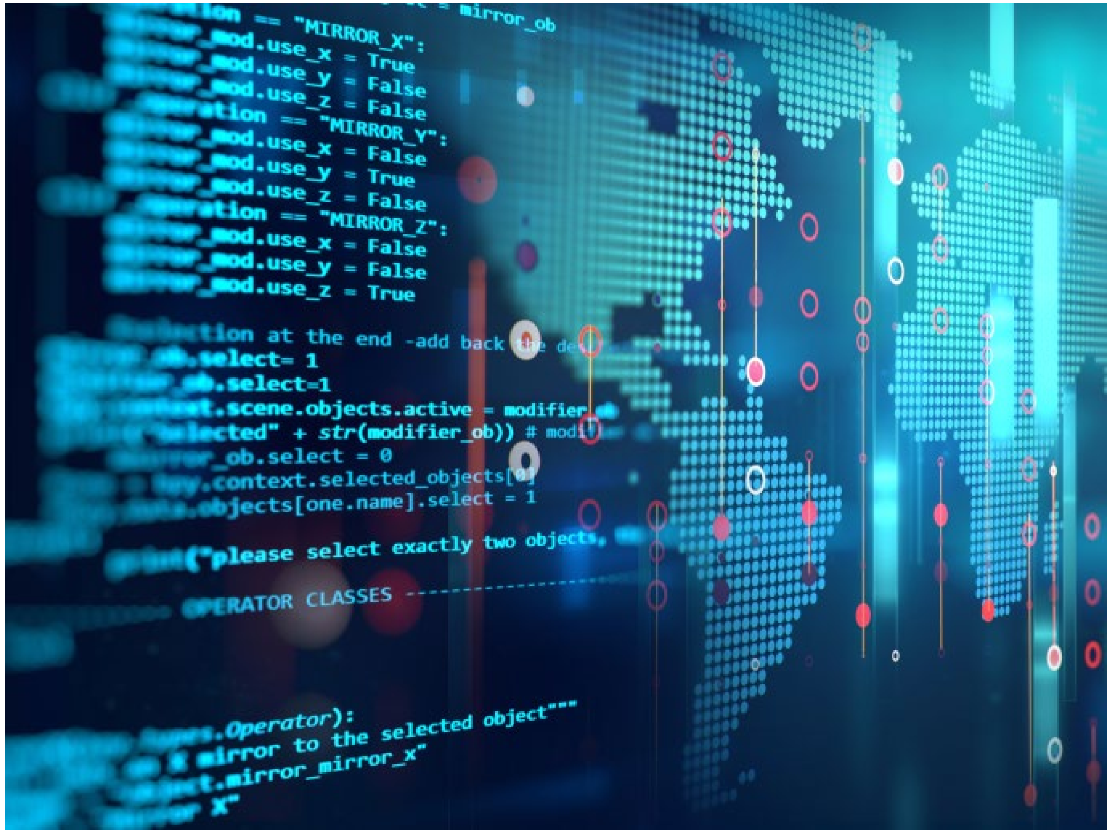
Quantum algorithms can find their way out of mazes exponentially faster than classical ones, at the cost of forgetting the paths they took. A new result suggests that the trade-off may be inevitable.

- “Quantum Algorithms and the Power of Forgetting”

- DC-QNet: Regional Quantum Network Testbed
  - Joint effort of NIST, NASA, NSA, ARL, NRL, USNO
  - Now operational
  - NIST focus: Quantum Network Metrology
  - Recent work: timing, synchronization, noise characterization



Encryption Updates: 3 New Draft FIPS



FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
(Crystals – Kyber)

FIPS 204, *Module-Lattice-Based Digital Signature Standard*
(Crystals – Dilithium)

FIPS 205, *Stateless Hash-Based Digital Signature Standard*
(Sphinx +)

NIST NCCoE Projects Kicking Off

Responding and Recovering from an ICS Cyber Attack

Developing practical guidance for manufacturers to respond and recover from a cybersecurity incident involving industrial control systems.

Water Cybersecurity

Developing practical guidance to reduce cybersecurity risks to water utilities.

Digital Identities – Mobile Driver's License

Developing practical guidance to implement mobile driver's license, focusing on the use case of using mDLs to meet customer identification/know your customer requirements for establishing a financial account.

Cybersecurity of Genomic Data

Developing the first joint NIST Cybersecurity and Privacy Framework Profile –tailoring our frameworks to apply to genomic data.

NIST – ITL And Workforce - NICE

Registration for the 2024 NICE Conference and Expo is now open! This year's theme, "**Strengthening Ecosystems: Aligning Stakeholders to Bridge the Cybersecurity Workforce Gap**," highlights the collective effort to strengthen the cybersecurity landscape. By joining forces with key partners, we can foster a more robust cybersecurity ecosystem to bridge the workforce gap.

NOTICE OF FUNDING OPPORTUNITY (NOFO)
Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development
Notification of Awards Expected to be Announced Soon

Staff Recognition

NIST Fellow:

- Mary Theofanos

Commerce Gold Medals:

- Dylan Yaga for improving law enforcement, DHS, and U.S. Border Patrol operations by identifying over 1,000 errors in biometric data exchange standards.
- Greg Cooksey, Paul Patrone, Anthony Kearsley, and Matthew DiSalvo for the invention of serial cytometry, a revolutionary technology for cancer diagnostics and therapeutic evalution.
- John Jones II, Karen Reczek, Allison Getz, Donna Sirk, Barbara Guttman, Marcela Najarro, Alan Zheng, Will Guthrie, and John Butler for extraordinary national leadership in improving the scientific quality of forensic practices through standards development
- Peter Bajcsy and Carl Simon, Jr. for developing a suite of tools used to characterize a first-of-its-kind tissue-engineered product for treatment of macular degeneration.

Staff Recognition

Commerce Silver Medals:

- Kristen Greene, Shanee Dawkins, Yee-Yin Choong, Mary Theofanos, Scott Ledgerwood, Kerrianne Buchanan, Susanne Furman, Kevin Mangold, and Adam Pintar ror giving a vital voice to U.S. first responders' communication technology needs in law enforcement, firefighting, and emergency services.
- Monique Hunter, Scott Jackson, Jason Kralj, Stephanie Servetas, and Blaza Toman for the development of a first-of-its-kind biologically stable water quality standard that modernizes recreational water surveillance.

NIST Bronze Medals:

- Ann Virts, Ya-Shian Li-Baboud, and David Schmitt for developing innovative metrics, test methods, artifacts, and datasets that measure the performance and safety of exoskeleton wearable robots.
- Julie Haney for leading and developing NIST’s Usable Cybersecurity Program, transforming how government agencies view the human element in cybersecurity.
- Martin Stevens, Ralph Jimenez, Charles H. Camp, Jr. and Thomas Gerrits for refuting published claims about quantum-enhanced microscopy by careful measurements of molecular absorption of photon pairs.
- Michael Indovina, Robert Snelick, John Garguilo, Andrew McCaffrey, and Sheryl Taylor for the creation of innovative software to help fight communicable diseases by ensuring that clinicians have accurate vaccine recommendations.
- Michael Nelson, Blaza Toman, David Newton, Johanna Camara, Lane Sander, Amanda Koepke, and Katrice Lippa for development and deployment of a statistical tool for experiment design and rigorous assessment of measurement uncertainty for chemical analysis.

Staff Recognition

NIST Bronze Medals:

- Nader Moayeri for collecting a set of BLE RSSI data and evaluating the performance of various proximity detection methods to blunt the spread of infectious diseases.

Director’s Award for Excellence in Administration:

- Melissa Banner et al for development of the Administrative Management Portal to centralize precise training and resources for the NIST administrative management community.

George Uriano Award:

- Timothy McBride, Sanjay Rekhi, et al for positioning NIST and DOC to successfully implement core CHIPS for America Act programs to revitalize US leadership in semiconductor manufacturing.

Judson C. French Award:

- Blaza Toman et al for development of the first glycan SRM for accurate quantification of N-linked glycans in monoclonal antibody therapeutics.

Ron Brown Excellence in Innovation Award:

- Greg Cooksey, Paul Patrone, Anthony Kearsley, and Matthew DiSalvo for pioneering real-time, cell-by-cell analysis for early cancer diagnosis, the evaluation of novel therapeutics, and accurate clinical decisions.

QUESTIONS?