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

NIST Information Technology Research

June 10, 2015

Charles Romine
ITL Director

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

Context

Strategic Drivers


Vision and Mission


Value to Stakeholders


Relevance to Industry


Relevance to National Priorities


Technology Environment

Value to Stakeholders

Globally Recognized and Trusted Source of Information

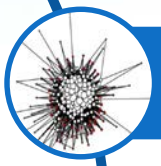
Reliable, Best-in-Class Expertise

Innovation Accelerator

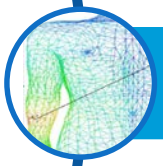
Agile in Addressing National Priorities

Technology Environment

IT Advances Quickly



IT is Intrinsically Complex

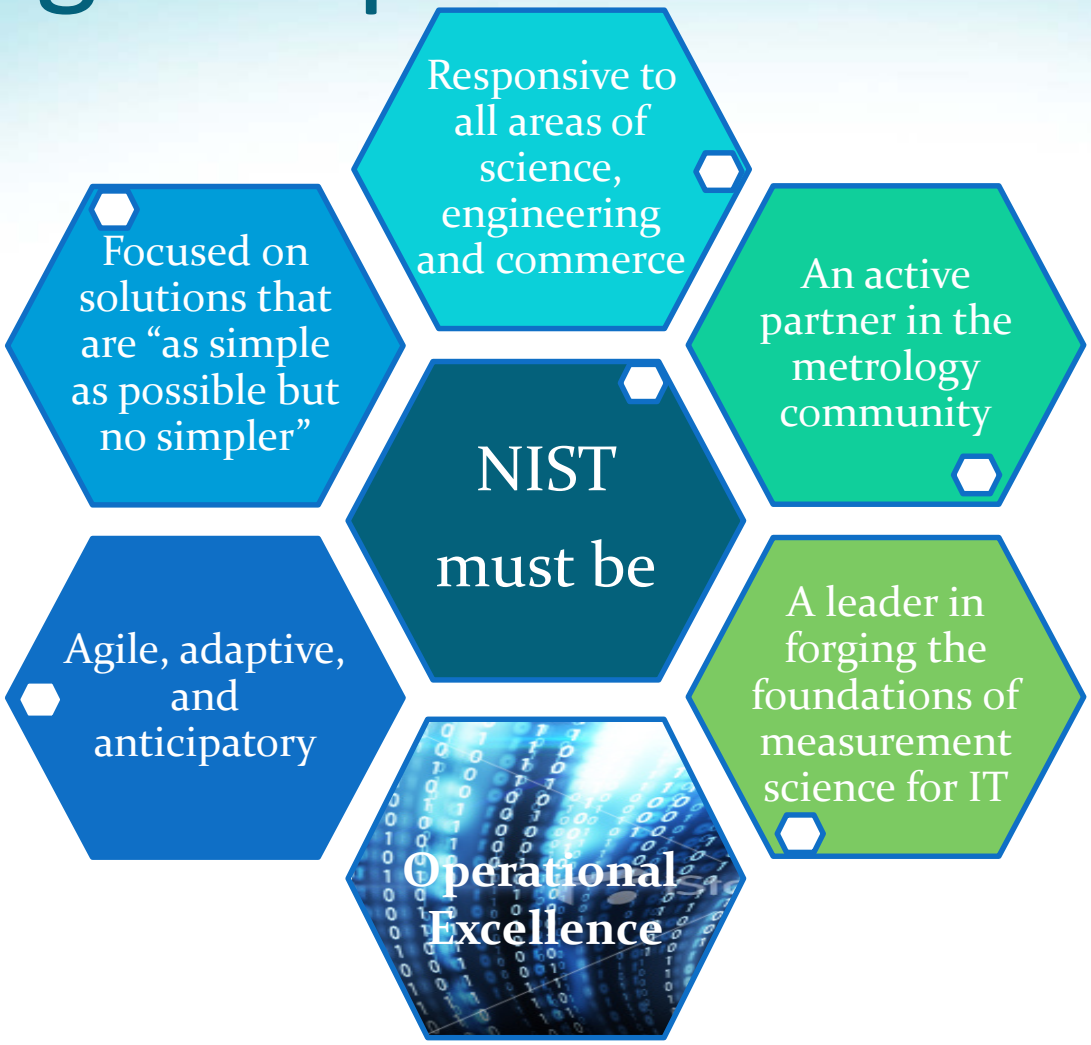


IT is Pervasive

Demand for IT in Measurement Science is Increasing

Measurement Science for IT is Still in Its Infancy

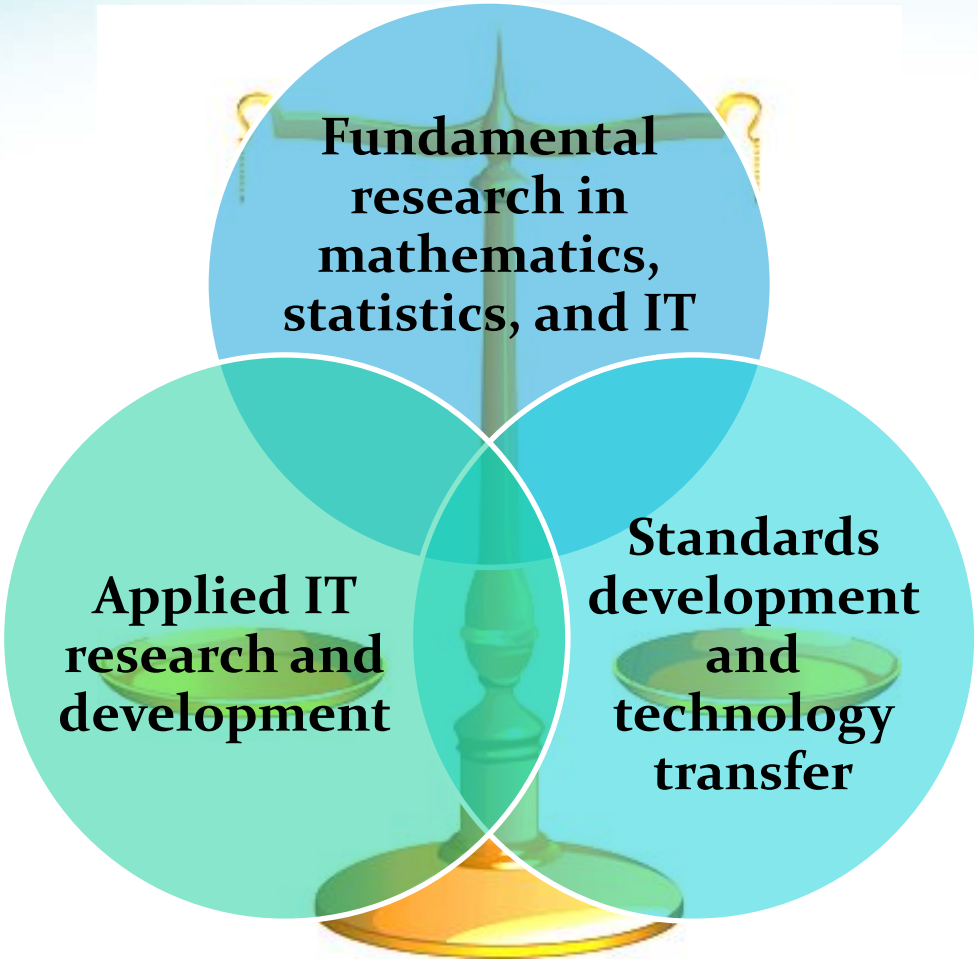
Strategic Implications

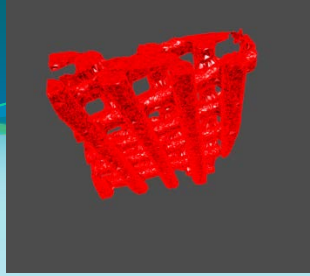


NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Strategy

Science and Engineering Strategy





Fundamental Research

Strategic Goal: *Develop the essential foundations of computer science, mathematics, statistics, and physical science that contribute to NIST's role in IT and measurement science.*

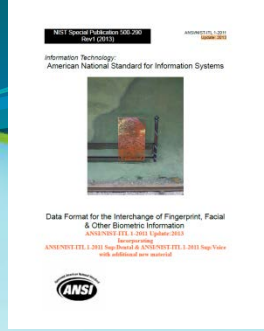
- Develop the Foundations of **Measurement Science for IT**
- Develop the Foundations of **IT for Measurement Science**

©Nick Macintosh

Applied Research

Strategic Goal: *Accelerate IT innovation through the development and application of measurements and related technology and tools.*

- Overcome Technical Barriers to IT Innovation
- Drive Progress on National Priorities
- Advance the NIST Mission



Standards Development & Technology Transfer

Strategic Goal: *Ensure the products of our research are available to all to promote U.S. innovation and industrial competitiveness, enhance economic security, and improve our quality of life.*

- Catalyze the Development of IT Standards
- Build Communities of Interest
- Outreach and Open Data Access

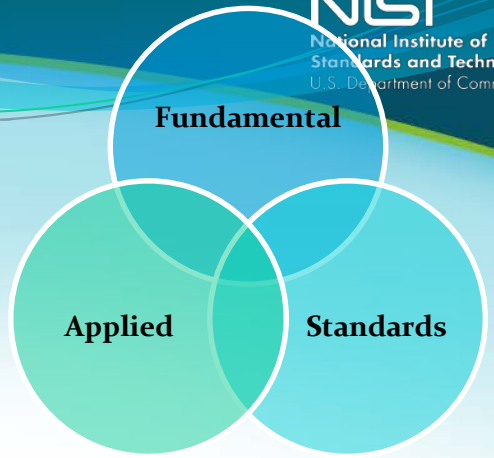
Partnerships Across Industry, State/ Local Governments and Academia

- National Cybersecurity Center of Excellence
- Identity Ecosystem Steering Group
- Joint Center for Quantum Information and Computer Science (QuICS)
- Big Data Public Working Group
- Cyber-Physical Systems Public Working Group
- Standards Developing Organizations

Key External Stakeholders

International collaborations

Priorities for Growth



Software Defined Networks

Cryptography

Big Data ★

Privacy

Software Assurance ★

Metrology for Scientific Computing ★

★ Discussed by Upcoming Internal Panel

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

Example Programs

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

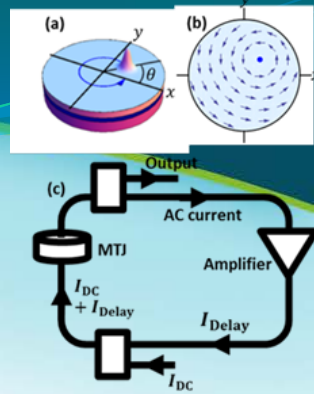
Fundamental Research

Quantum Information Science

iTL PML

QIS can, in theory, enable phenomenal increases in computing capability and provably secure communication channels

- Improve understanding of the potential of QIS to revolutionize IT
- Enable mitigation of the threat posed to public key crypto-systems
- Develop measurement infrastructure for future IT products based on quantum technologies
- Established the Center for Quantum Information and Computer Science (QuICS), a joint venture of NIST, UMD, and the NSA



Fundamental Research

Spintronics for biologically inspired computing

Use spintronics devices to perform biologically-inspired computing, such as reservoir computing or associative memories

Bio-inspired computing takes inspiration from the processes the brain uses to design processors that accomplish similar tasks with much lower power.

Spintronic devices operating at low power can capture many of the behaviors of neurons and synapses offering one path to such computational engines

Carried out preliminary calculations testing the suitability of spin-torque nano-oscillators to serve as the active device in a reservoir computer

CNST
Center for Nanoscale Science & Technology

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

Applied Research

Cyber-Physical Systems/Internet of Things

Through new measurement science, advanced testbed capabilities, and community-based efforts, enable the scalable design and reproducible performance measurement of advanced Cyber-Physical Systems

Cyber-Physical Systems Public Working Group

Global City Teams Challenge: enhance the livability, workability and sustainability of communities

5 subgroups in reference architectures, use cases, cybersecurity, timing, and data

The first-ever CPS Framework is expected to be released for public comments in July

Encourage cities, innovators, and researchers to deploy standards-based smart city solutions

24+ cities across the globe are collaborating with 200+ companies and universities

Applied Research

Cybersecurity

Conduct research, development and outreach necessary and provide standards and guidelines, mechanisms, tools, metrics and practices *to protect* our nation's information and information systems

- Standards, Guidelines, Best Practices
- Cybersecurity Framework (EO 13636)
- Cryptography
- Risk Management
- Cybersecurity for Smart Manufacturing Systems
- Completed a major update of the Guide to Industrial Control System (ICS) Security
- National Strategy for Trusted Identities in Cyberspace
- New Pilot Program in Privacy
- National Cybersecurity Center of Excellence
- Established the Nation's only FFRDC dedicated to cybersecurity
- National Initiative for Cybersecurity Education
- Developed Cybersecurity Workforce Framework

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

MML iTL engineering laboratory

Applied Research

Materials Genome Initiative

The interagency Materials Genome Initiative aims to reduce time & cost to discover, develop, manufacture, and deploy advanced materials

- Develop methods and tools for the computer representation and interchange of materials data
- Develop open software platforms for materials modeling
- Develop analyses of novel materials models
- Develop methods for verification, validation and uncertainty quantification for materials models and simulations
- Released the Materials Data Curation System an extensible tool for managing materials measurement data

Standards Development & Tech Transfer

Biometrics

Develop measurement and evaluation methods and standards to advance the use of image-based biometric technologies

ANSI/NIST-ITL, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*

- Fingerprint, palm print, facial/ mugshot, iris
- Scar, Mark & Tattoo
- DNA and Footprints
- Extended Feature Set
- Geo-positioning coordinates of biometric sample collection
- Forensic & Investigatory Voice
- Dental Forensics

Influencing a Multi-Trillion Dollar Industry

- Biometrics
- Cloud Computing
- Cryptography
- Digital Library of Mathematical Functions
- Domain Name Security (Advanced Networking)
- Health IT

Questions

Panel of Internal Speakers

- Metrology for Scientific Computing – Andrew Dienstfrey
- Big Data and Data Science – Mark Przybocki
- Software Quality – Paul Black

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

Background: IT-related Mandates

Specific Mandates (1 of 4)

- Biometrics
  - USA PATRIOT Act
  - Enhanced Border Security and Visa Entry Reform Act
  - Homeland Security Presidential Directive #12: Policy for a Common Identification Standard for Federal Employees and Contractors
  - 10-Print Transition: mandated by Homeland Security Council Deputies Committee
  - National Security Presidential Directive/Homeland Security Presidential Directive (NSPD-59/ HSPD-24), Biometrics for Identification and Screening to Enhance National Security
- Cloud Computing
  - America COMPETES Reauthorization Act of 2010
  - Federal Cloud Computing Strategy (February 2011)

Specific Mandates (2 of 4)

- DNSSEC
  - OMB Memo M-08-23
- Healthcare
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
- Cybersecurity
  - Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283) supersedes Federal Information Security Management Act of 2002 (Title III of the E-Government Act), including Information Security and Privacy Advisory Board (ISPAB) mandate amended
  - Cybersecurity Enhancement Act of 2014 (Public Law 113-274)
  - Improving Critical Infrastructure Cybersecurity (Executive Order 13636 , February 12, 2013)
  - National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23): Comprehensive National Cybersecurity Initiative
    - National Initiative for Cybersecurity Education

Specific Mandates (3 of 4)

- Cybersecurity, continued
  - Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) [supersedes Computer Security Act of 1987 (Public Law 100-235)]
  - Computer Security Research and Development Act of 2002
  - Homeland Security Presidential Directive #12
  - Conference Report on House Resolution 5441, Department of Homeland Security Appropriations Act, 2007: Title V - General Provisions (WHTI Certification effort)
  - OMB M04-04 E-Authentication Guidance for Federal Agencies
  - Information Technology Management Reform Act of 1996, Public Law 104-106
  - OMB Circular A-130 and OMB Directive 05-24
  - National Cybersecurity Center of Excellence (Public Law 112-55, Consolidated and Further Continuing Appropriations Act of 2012)

Specific Mandates (4 of 4)

- Identity Management
  - National Strategy for Trusted Identities in Cyberspace
- Internet Protocol version 6 (IPv6)
  - OMB Memo on Transition to IPv6 (September 28, 2010)
  - OMB Memo M-05-22 on Transition Planning for IPv6 (August 2, 2005)
- Smart Grid
  - Energy Independence and Security Act (EISA) of 2007
  - American Recovery and Reinvestment Act of 2009
- Voluntary Voting System Standards
  - Help America Vote Act
  - Military and Overseas Voter Empowerment (MOVE) Act of 2009