NIST

Dr. Susan F. Zevin

Acting Director
Information Technology Laboratory (ITL)
National Institute of Standards and Technology (NIST)
February 2, 2003

Outline

- NIST/ITL Overview
- Where NIST Fits In....
- Importance of Standards/Certification
- The Big Picture

National Institute of Standards and Technology

NIST Assets Include:

NIST Laboratories -- National measurement standards

- 3,000 employees
- 1,500 technical staff
- 1,600 guest researchers
- Unique measurement and research facilities
- Joint institutes with universities

Extramural programs

- Advanced Technology Program -- $640 million current R&D partnerships with industry
- Manufacturing Extension Partnership -- 400 centers nationwide
- Baldrige National Quality Award

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

NIST Products and Services

- Measurement Research

  2,200 publications/year
- Standard Reference Data

  65 types available

  5,000 units sold/ year
- Standard Reference Materials

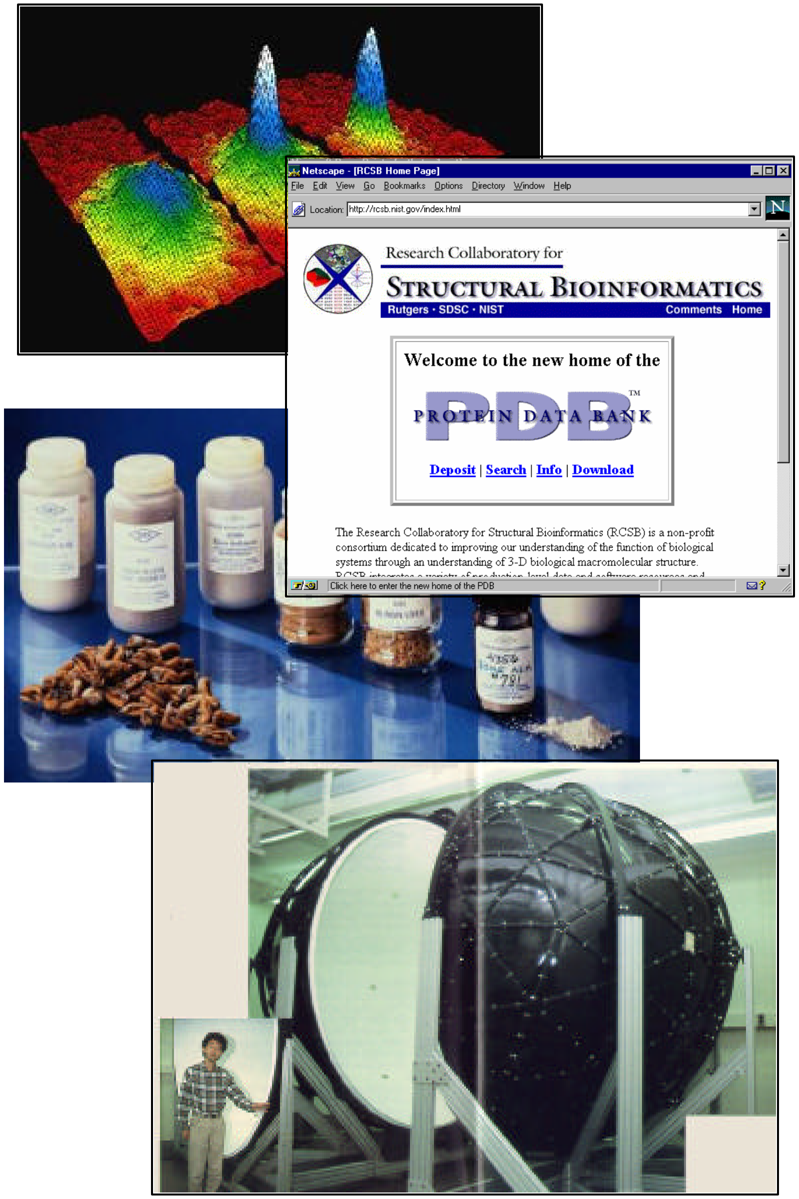
  >1,300 products available

  30,000 units sold/year
- Calibrations and Tests

  >3,000 items calibrated/year
- Laboratory Accreditation

  764 accreditations
- Standards Committees

  400 NIST staff, 900 committees

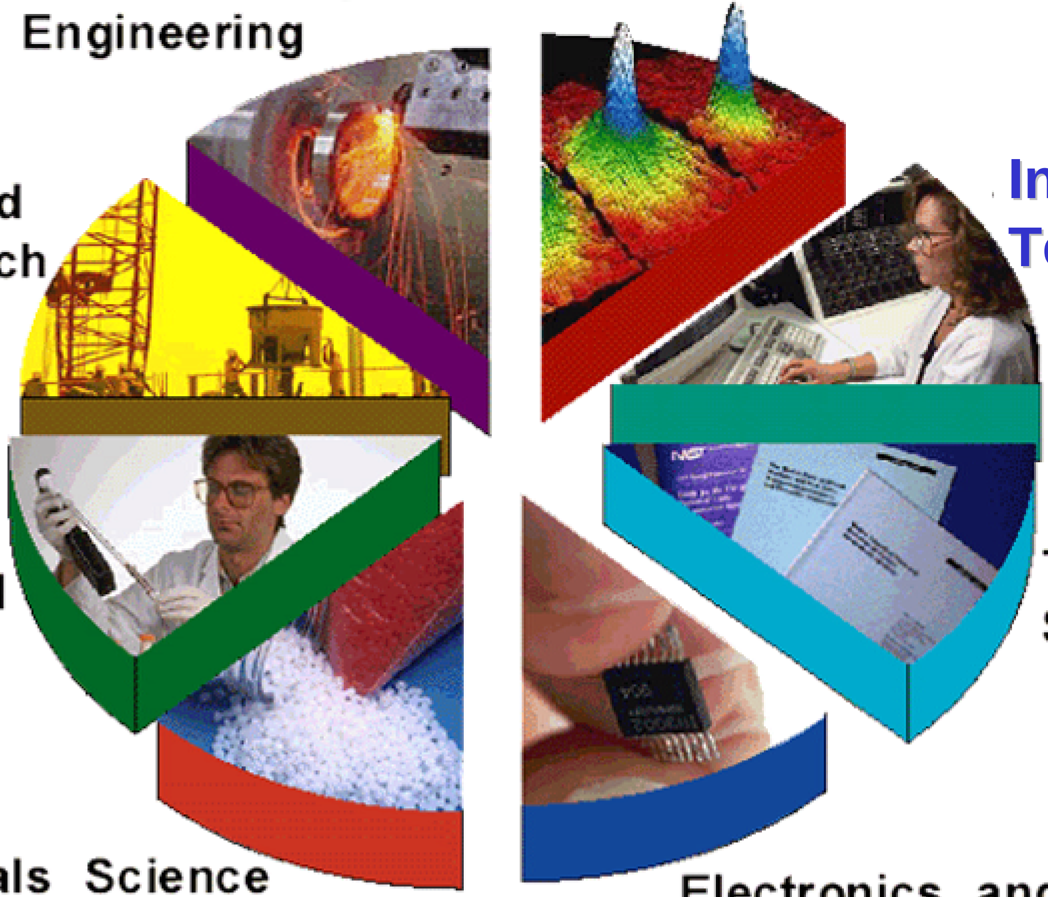

Netscape - [RCSB Home Page]
File Edit View Go Bookmarks Options Directory Window Help
Location: http://rcsb.nist.gov/index.html
Research Collaboratory for
Structural Bioinformatics
Rutgers · SDSC · NIST
Comments Home
PDB™
PROTEIN DATA BANK
Click here to enter the new home of the PDB

Welcome to the new home of the

Deposit | Search | Info | Download

The Research Collaboratory for Structural Bioinformatics (RCSB) is a non-profit consortium dedicated to improving our understanding of the function of biological systems through an understanding of 3-D biological macromolecular structure.

NIST's Measurement and Standards Laboratories



Manufacturing Engineering

Physics

Building and Fire Research

Information Technology

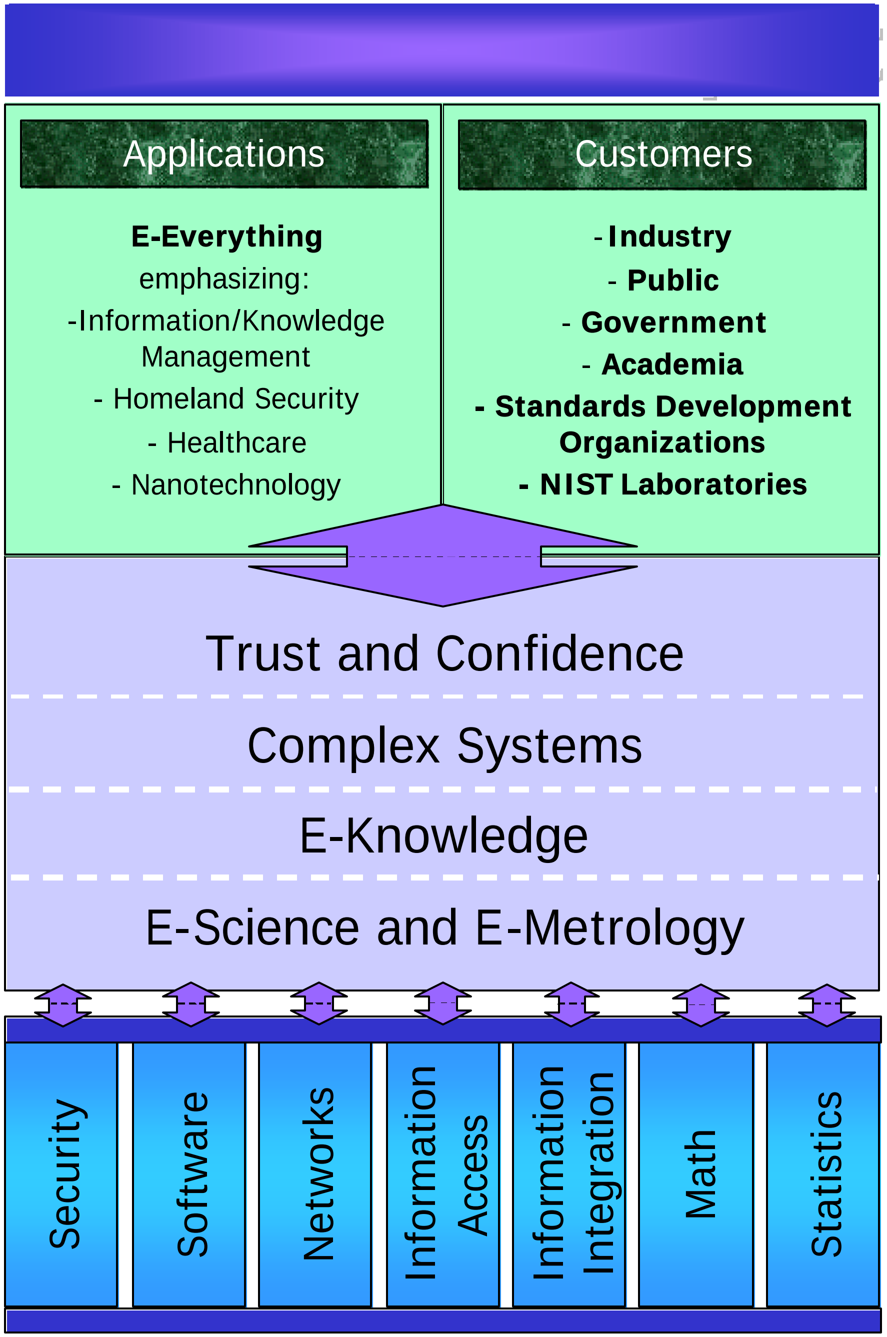
Chemical Science and Technology

Technology Services

Materials Science and Engineering

Electronics and Electrical Engineering

NIST
National Institute of Standards and Technology



Applications

E-Everything

emphasizing:

-Information/Knowledge Management

- Homeland Security

- Healthcare

- Nanotechnology

Customers

- Industry

- Public

- Government

- Academia

- Standards Development Organizations

- NIST Laboratories

Trust and Confidence

Complex Systems

E-Knowledge

E-Science and E-Metrology

Security

Software

Networks

Information Access

Information Integration

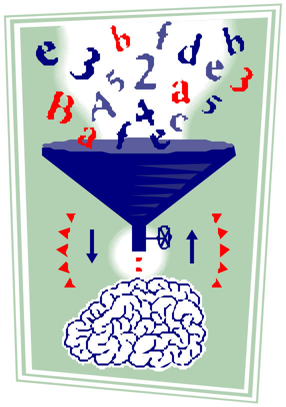
Math

Statistics

Where NIST Fits In…

Trust and Confidence

- Motivation -



Customers Ask:

Is the IT system doing what I expect?

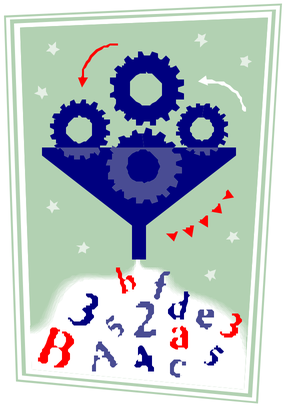
Has the data been tampered with?

Am I acquiring the relevant data?

Will data be available when I need it?

Are my measurements provably correct?

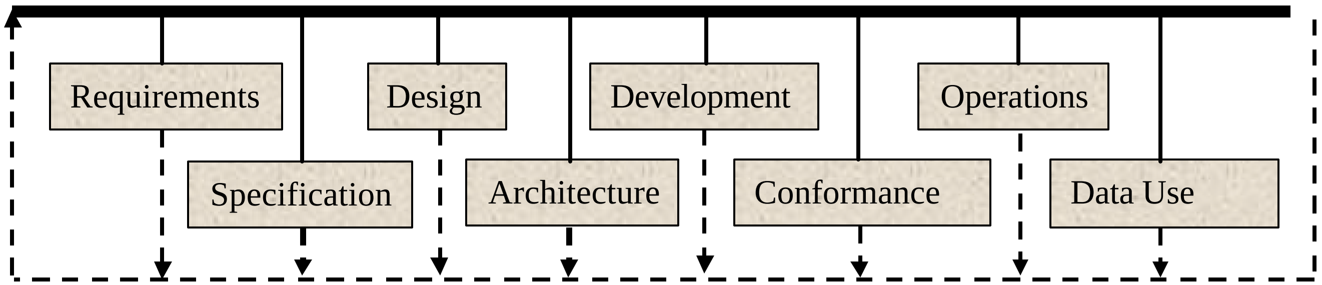
Can I use information to speed development?



NIST Approach to Standards

- Collaboration with industry to define and demonstrate a framework and prototype
  - Can be adopted and extended by others
- Work with the community
  - Identify stakeholders, roles, use cases
  - Identify relevant standards, organizations
  - Identify existing and similar efforts
- Define the metadata, taxonomies, and information model
- Develop framework infrastructure and web services
- Demonstrate and deploy

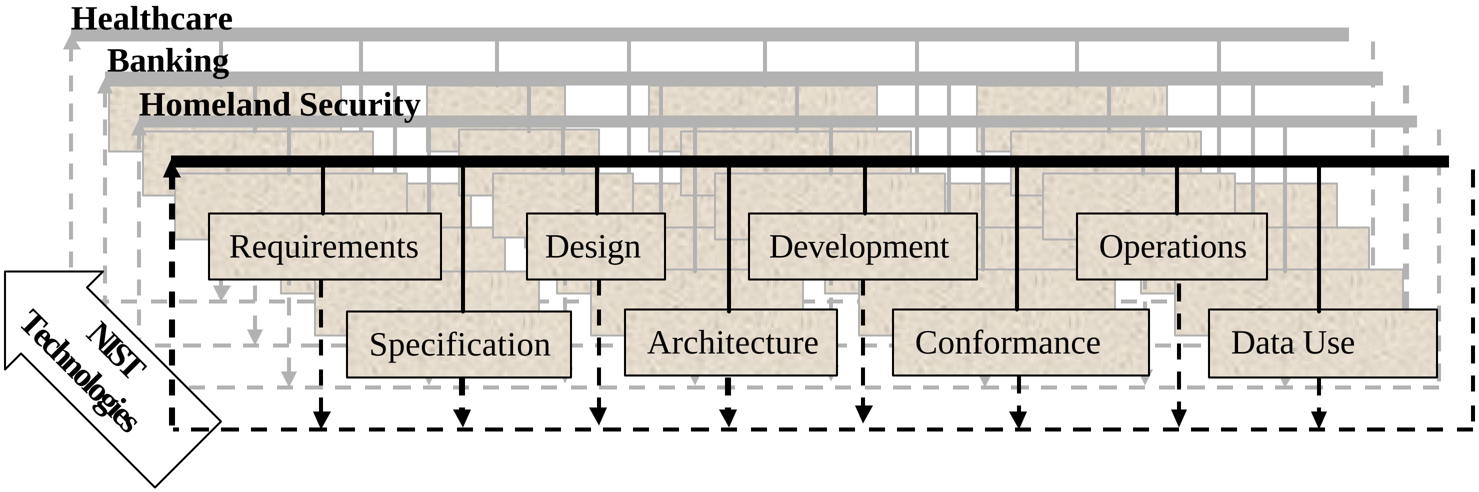
Trust and Confidence Continuum



Term	Definition*	Level of Measurement Science Development
Requirement	Demanded, obligatory	Undeveloped
Specification	Statement of particulars	Underdeveloped
Design	Conceive in the mind, plan	Underdeveloped
Architecture	Science of building	Underdeveloped
Development	Act, process or result of developing	Underdeveloped
Conformance	Acting in accord	Underdeveloped
Operations	Performance of work	Developed
Preservation	Protect and maintain	Underdeveloped

* Synopsis of definitions found in Webster's II: New Riverside University Dictionary

NIST Technologies – Across Boundaries



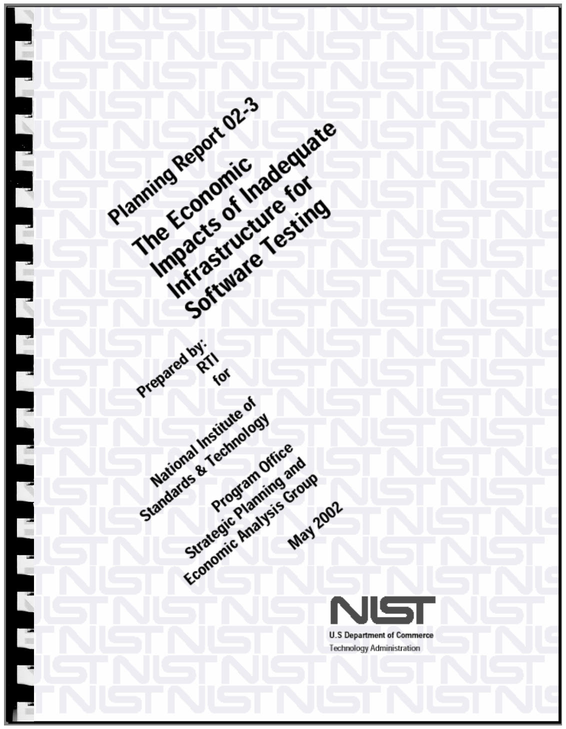
National Institute of Standards and Technology

Importance of Standard Approaches to Testing

National Institute of Standards and Technology

Software Testing Study

- Costs of inadequate infrastructure for software testing is estimated at $59.5 billion
- Potential cost reduction from feasible infrastructure improvements is $22.2 billion



Planning Report 02-3

The Economic Impacts of Inadequate Infrastructure for Software Testing

Prepared by:
RTI
for

National Institute of Standards & Technology

Program Office
Strategic Planning and
Economic Analysis Group

May 2002

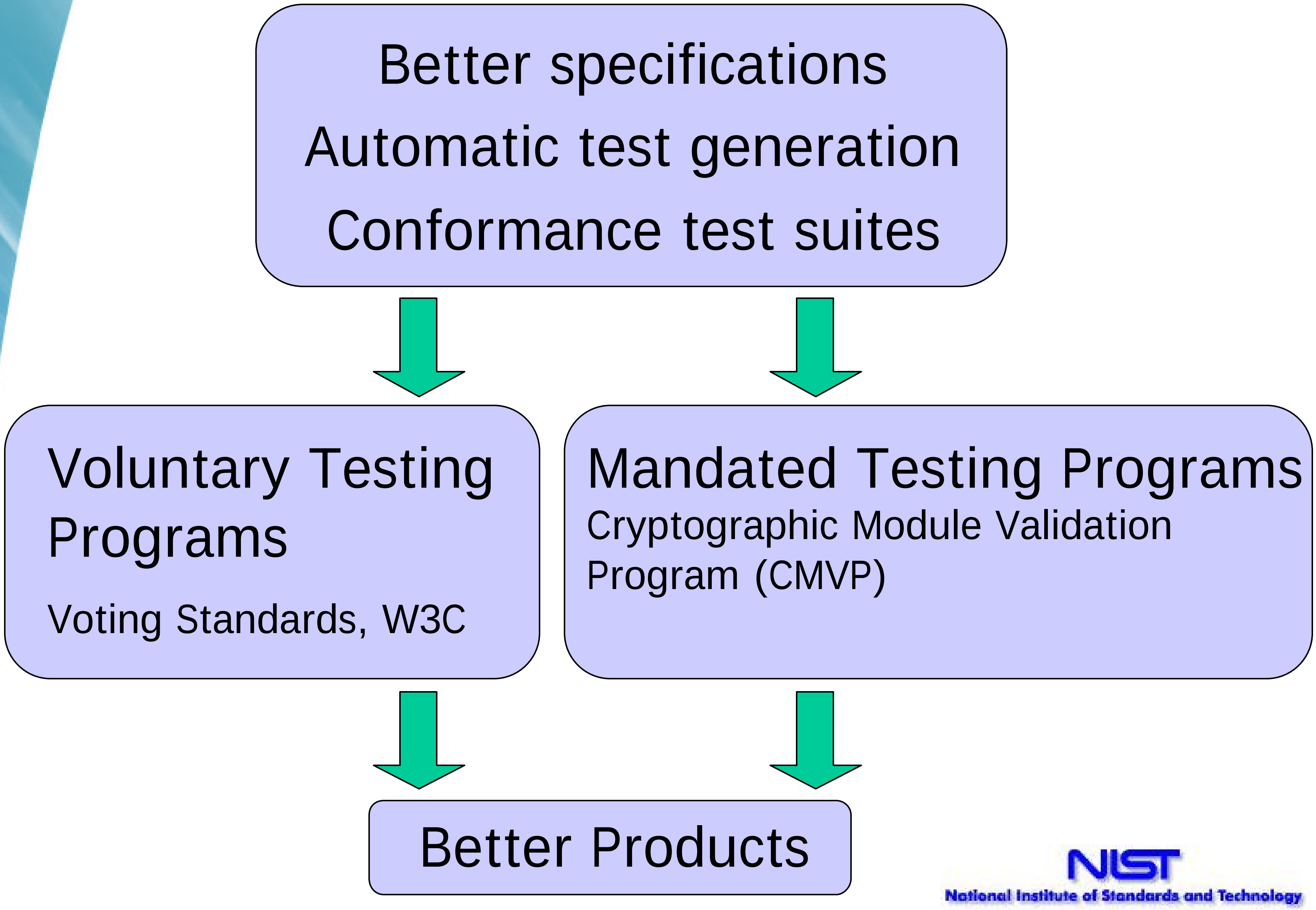
NIST
U.S Department of Commerce
Technology Administration

"total sales of software approximately $180 billion"

"half of the costs are borne by users"

National Institute of Standards and Technology

Ways to improve...



Better specifications

Automatic test generation

Conformance test suites

Voluntary Testing Programs

Voting Standards, W3C

Mandated Testing Programs

Cryptographic Module Validation Program (CMVP)

Better Products

NIST

National Institute of Standards and Technology

Certification Case Study

Voting Systems

- Independent, non-Federal lab applies to NIST
- NIST certifies Accredited Lab
- Independent Testing Authority (ITA) applies to Accredited Laboratory
- Accrediting Lab uses ISO 17025 to analyze ITA
- ITA Certified
- Vendor sends voting system to ITA for testing
- ITA performs testing and certifies voting system against the voting system standards

Certification Case Study

CMVP – Cryptographic Module Validation Program

Validation testing for cryptographic modules and algorithms against Federal Information Processing Standards

Initial survey of the testing of the first 164 cryptographic modules and 332 algorithm validations that were validated

Question: does the CMVP testing reveal any underlying flaws in completed ready to market modules that were submitted for testing.

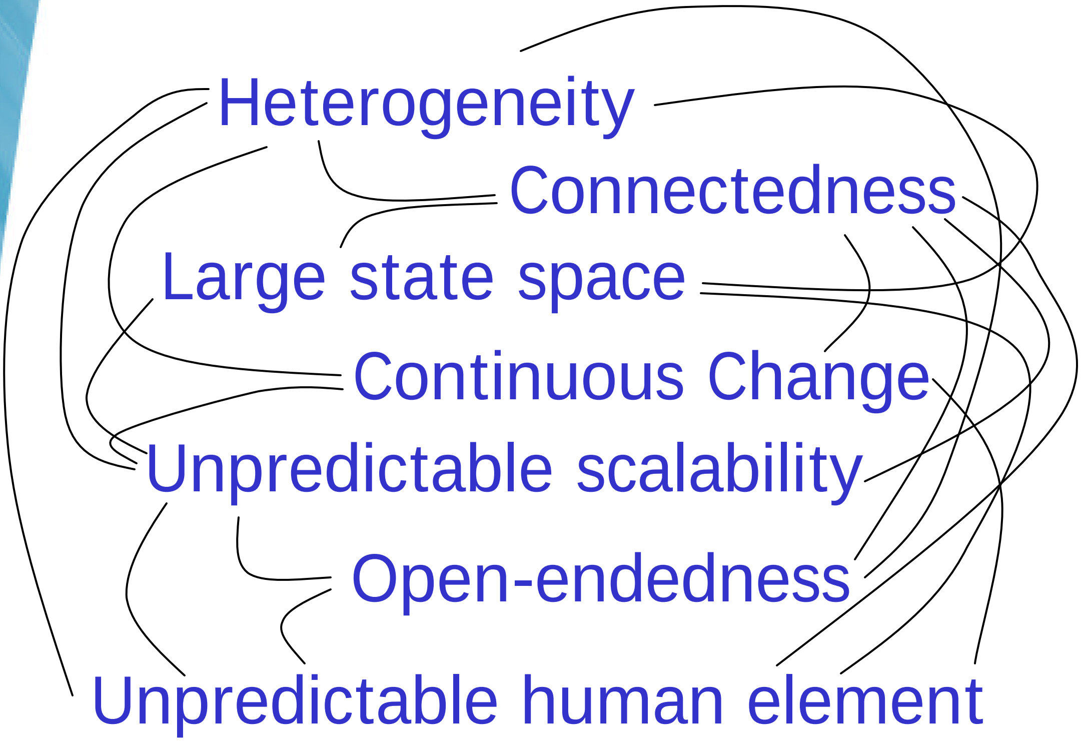
Results:

Cryptographic modules: 80 security flaws were discovered, and 158 documentation errors were found

Algorithm validations: 88 security flaws and 216 documentation errors were found

Understanding and Control of Complex Systems

The interconnected characteristics of a complex system need...



Heterogeneity

Connectedness

Large state space

Continuous Change

Unpredictable scalability

Open-endedness

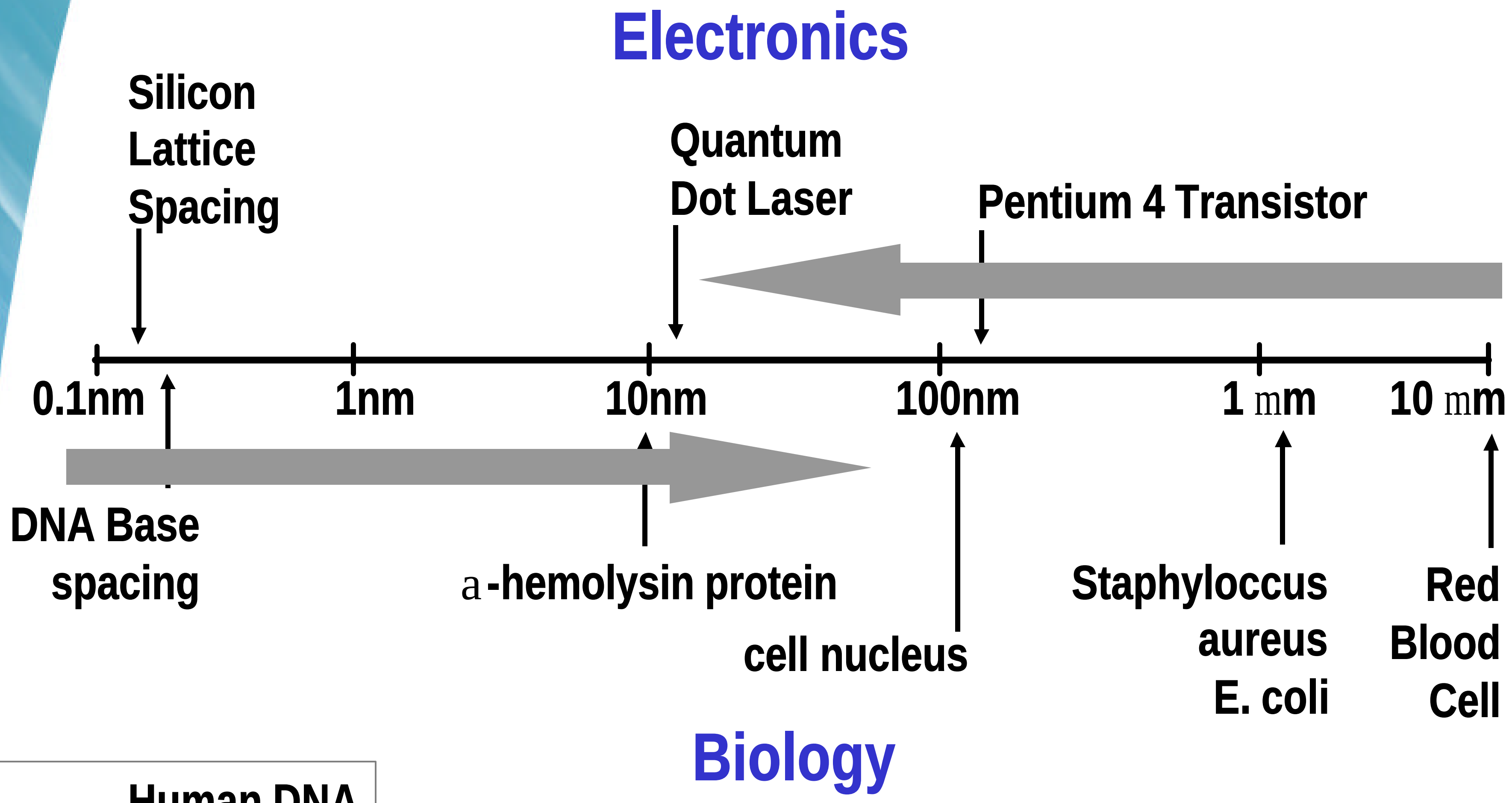
Unpredictable human element

...Systems level understanding with certain component and system characteristics

- Real-time
- Self-adaptive
- Self-organizing
- Self-healing
- Self-forming
- Self-testing
- Resilient, etc

NIST
National Institute of Standards and Technology

Spatial Resolution



Electronics

Silicon Lattice Spacing

Quantum Dot Laser

Pentium 4 Transistor

0.1nm

1nm

10nm

100nm

1 mm

10 mm

DNA Base spacing

a -hemolysin protein

cell nucleus

Staphyloccus aureus E. coli

Red Blood Cell

Biology

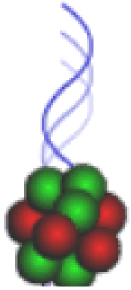
Human DNA
3 billion base pairs
1 meter total length

Smaller: Quantum Information Science

Confluence of two revolutions of the 20th century: *computer science and quantum physics*

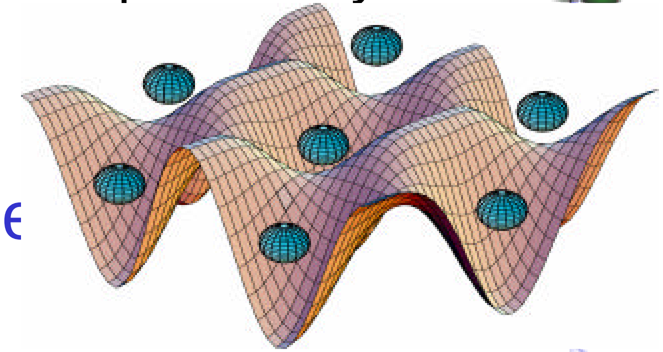
Paradigm shift: information as a physical quantity

NBS SEAC, 1950



Implications for homeland security

- Perfectly secure defense communications
- Ability to solve problems impossible to compute today
  - Codebreaking
  - Pattern matching

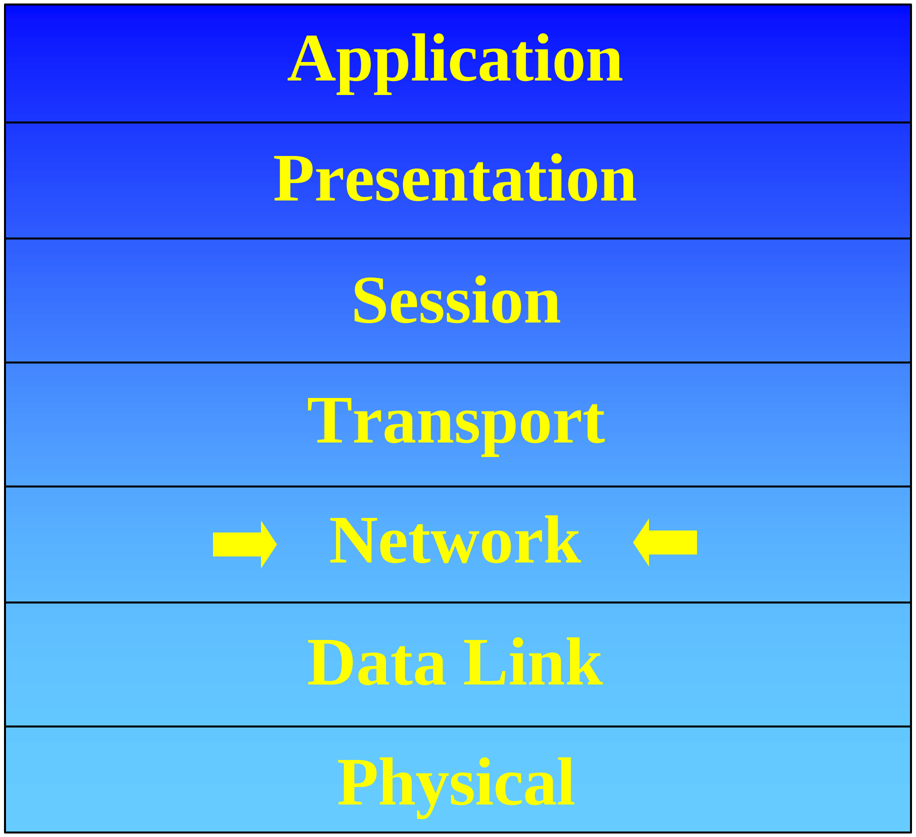


Implications for commerce and trade

- Secure electronic commerce
- Maintenance of lead in computer technology marketplace

NIST
National Institute of Standards and Technology

Don’t Forget the Big Picture...



Application

Presentation

Session

Transport

➡ Network ⬅

Data Link

Physical