NIST's Mission & NMI Role

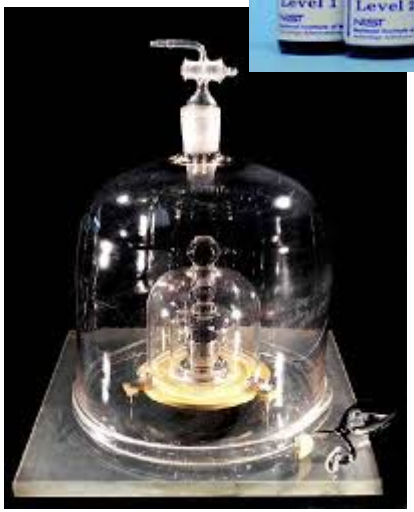
- NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

- NIST is the national metrology institute (NMI) for the United States. As an NMI, NIST
  - Maintains primary measurement standards for the seven base units in the SI system of units and for derived units
  - Offers calibration services and measurement standards to support international trade
  - Develops new measurement technologies

Locations

- Primary sites
  - Gaithersburg, MD
  - Boulder, CO
- Joint Research Institutes/Centers
  - DC/Boulder areas
  - Charleston, SC
  - Palo Alto, CA
  - Ames, IA
  - Chicago, IL
- WWV and WWVH
  - Fort Collins, CO
  - Kauai, HI

NIST Documentary and Physical Standards



FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.202

August 2015

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

INFORMATION TECHNOLOGY LABORATORY

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

IT Standards and Research

NIST | NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index | Search

Information Technology Portal

Publications | Subject Areas | Products/Services | NIST Organization | News | Programs & Projects | User Facilities | Work with NIST

NIST Home > Information Technology Portal

Information Technology Portal - Overview

Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, the National Institute of Standards and Technology accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

Cybersecurity Framework >>

Cloud Computing >>

Computer Security Resource Center >>

Information Technology Laboratory >>

National Cybersecurity Center of Excellence (NCCoE) >>

Smart Grid >>

National Strategy for Trusted Identities in Cyberspace (NSTIC) >>

Subject Areas

Biometrics

Select Language * SHARE

Powered by Google Translate

New NIST Security Standard Can Protect Credit Cards, Health Information 1 2 3 4

News And Events

NSCI Seminar: New Technologies for Improved Computer Performance

NSCI Seminar: An Overview of High Performance Computing and Benchmark Changes for the Future

IT Standards and Research

Software Testing Metrics

Telecommunications/Wireless

Programs and Projects

Measurement Science for Complex Information Systems
This project aims to develop and evaluate a coherent set of methods to understand behavior in complex information systems, such as the Internet, … **more**

Lightweight Cryptography Project
NIST is investigating the need for lightweight cryptographic algorithms. This includes looking at applications that may require lightweight … **more**

Video Analytics
The Multimodal Information Group's (MIG) video analytics program includes several activities contributing to the development of technologies that … **more**

Interdisciplinary Projects
Some Multimodal Information Group project areas span across multiple research areas within the group or to other groups in IAD. These … **more**

Advanced Video and Signal Based Surveillance
The Second Multiple Camera Single Person Tracking Challenge Evaluation (MCSPT) was held in conjunction with the 7th Advanced Video and Signal … **more**

Speaker and Language Recognition Projects
Our Speaker and Language Recognition program includes several activities contributing to speaker and language recognition technology and metrology … **more**

Video Playlist

Related Links

Budget in Brief FY 2013 - National Strategy for Trusted Identities in Cyberspace

Contact

General Information:
301-975-NIST (6478)
inquiries@nist.gov

100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070

Challenges in Measuring Software

- Physical quantities
  - regulated by physical laws and environments
  - measurements follow “nice” probability distributions (e.g. Gaussian, Poisson)
- Software
  - largely produced in human imagination, with some mathematical limits
  - measurements not purely deterministic or random
  - probability distributions may not be “nice” (e.g. multimodal, extremely skewed)

Need for Reliable Software

- Despite challenges, software has a critical impact on the economy and government
  - electronic commerce
  - identification of business trends/intelligence
  - delivery of health care
  - tracking disease spread
  - management of transportation systems
  - criminal investigations
  - product design
  - projecting climate trends

Today's Workshop

NIST Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities

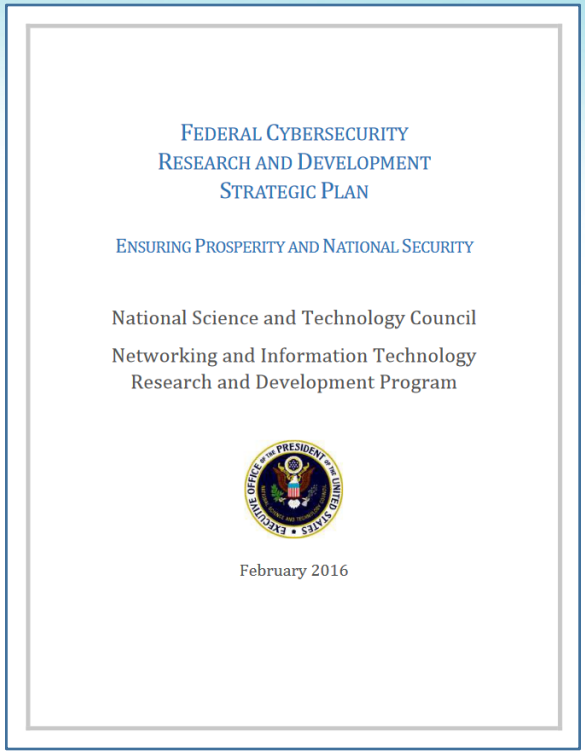
Purpose:

The Federal Cybersecurity Research and Development Strategic Plan seeks to fundamentally alter the dynamics of security, reversing adversaries' asymmetrical advantages. Achieving this reversal is the mid-term goal of the plan, which calls for "sustainably secure systems development and operation." Part of the mid-term (3-7 years) goal is "the design and implementation of software, firmware, and hardware that are highly resistant to malicious cyber activities ..." and reduce the number of vulnerabilities in software by orders of magnitude. Measures of software play an important role.

Industry requires evidence to tell how vulnerable a piece of software is, what techniques are most effective in developing software with far fewer vulnerabilities, determine the best places to deploy countermeasures, or take any of a number of other actions. This evidence comes from measuring, in the broadest sense, or assessing properties of software. With useful metrics, it is straight-forward to determine which software development technologies or methodologies lead to sustainably secure systems.

The goal of this workshop is to gather ideas on how the Federal Government can best use taxpayer money to identify, improve, package, deliver, or boost the use of software measures and metrics to significantly reduce vulnerabilities. We call for position statements from one to three paragraph long. Position statements may be on any subject like the following:

- existing measures of software that can make a difference in three to seven years,
- means of validating software measures or confirming their efficacy (meta-measurements),
- quantities (properties) in software that can be measured,
- standards (in both étalon and norme senses) needed for software measurement,
- cost vs. benefit of software measurements,



- surmountable barriers to adoption of measures and metrics,
- areas or conditions of applicability (or non-applicability) of measures,
- software measurement procedures (esp. automated ones), or
- sources of variability or uncertainty in software metrics or measures.

The output of this workshop and other efforts is a plan for how best the Federal Government can employ taxpayer money to significantly curtail software vulnerabilities in the mid-term.