Overview of
NIST Information Technology Laboratory

Software Assurance Forum
"Rugged Software"

Jim St. Pierre, Deputy Director,
Information Technology Laboratory
The National Institute of Standards
and Technology

March 1st, 2011

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

NIST - The View from 10,000 ft.

- The Nation's National Measurement Laboratory
- Central Mission: Support industry innovation
- Extremely broad research portfolio
- Established in 1901 – Nation's oldest physical science laboratory
- Where Nobel Prize science meets real world engineering
- World class facilities, national networks, international reach

NIST Mission and Programs

"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 Laboratories

- Create critical measurement solutions and promote equitable standards to stimulate innovation, foster industrial competitiveness, and improve the quality of life.

Hollings Manufacturing Extension Partnership

- Nationwide network of resources helping smaller manufacturers compete globally

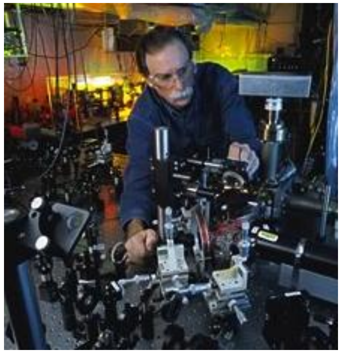
Baldrige Performance Excellence Program

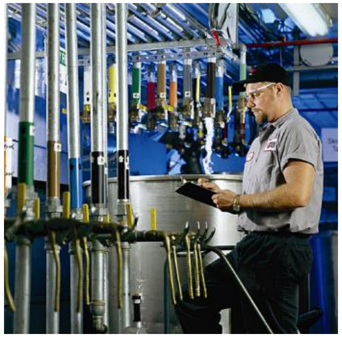
- Promoting and recognizing performance excellence via information and Presidential awards in manufacturing, service, small business, education, health care, and the nonprofit sector

Technology Innovation Program

- Supports development of cutting edge technologies by the private sector and universities to address critical national needs and key societal challenges

NIST is the nation's innovation agency

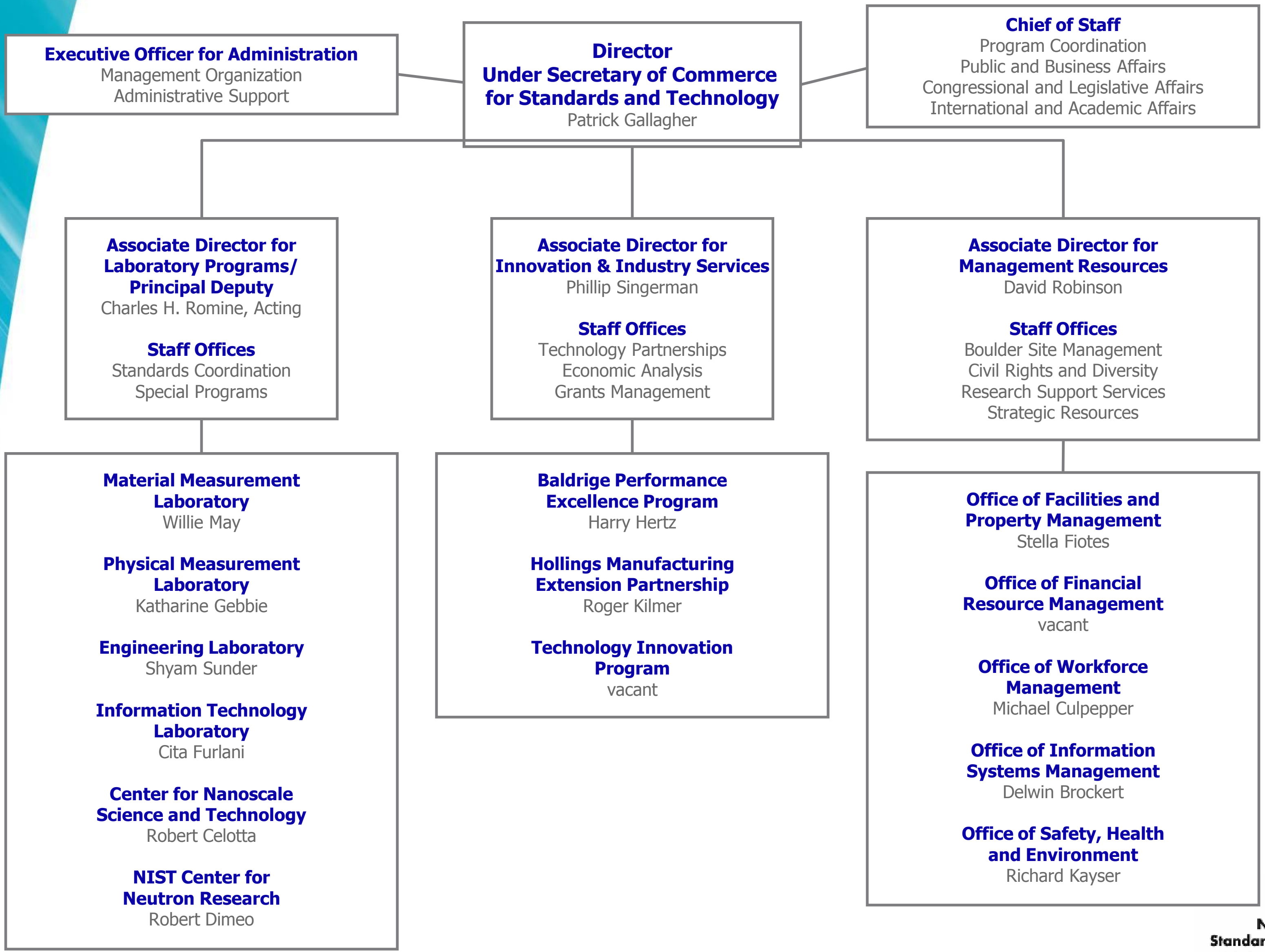

© Geoffrey Wheeler


Courtesy Stoner Inc.

Courtesy Steuben

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

NIST Realignment



Executive Officer for Administration
Management Organization
Administrative Support

Director
Under Secretary of Commerce for Standards and Technology
Patrick Gallagher

Chief of Staff
Program Coordination
Public and Business Affairs
Congressional and Legislative Affairs
International and Academic Affairs

Associate Director for Laboratory Programs/ Principal Deputy
Charles H. Romine, Acting

Staff Offices
Standards Coordination
Special Programs

Associate Director for Innovation & Industry Services
Phillip Singerman

Staff Offices
Technology Partnerships
Economic Analysis
Grants Management

Associate Director for Management Resources
David Robinson

Staff Offices
Boulder Site Management
Civil Rights and Diversity
Research Support Services
Strategic Resources

Material Measurement Laboratory
Willie May

Physical Measurement Laboratory
Katharine Gebbie

Engineering Laboratory
Shyam Sunder

Information Technology Laboratory
Cita Furlani

Center for Nanoscale Science and Technology
Robert Celotta

NIST Center for Neutron Research
Robert Dimeo

Baldrige Performance Excellence Program
Harry Hertz

Hollings Manufacturing Extension Partnership
Roger Kilmer

Technology Innovation Program
vacant

Office of Facilities and Property Management
Stella Fiotes

Office of Financial Resource Management
vacant

Office of Workforce Management
Michael Culpepper

Office of Information Systems Management
Delwin Brockert

Office of Safety, Health and Environment
Richard Kayser

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

ITL Mission

To promote US innovation and industrial competitiveness by advancing

measurement science,

standards, and

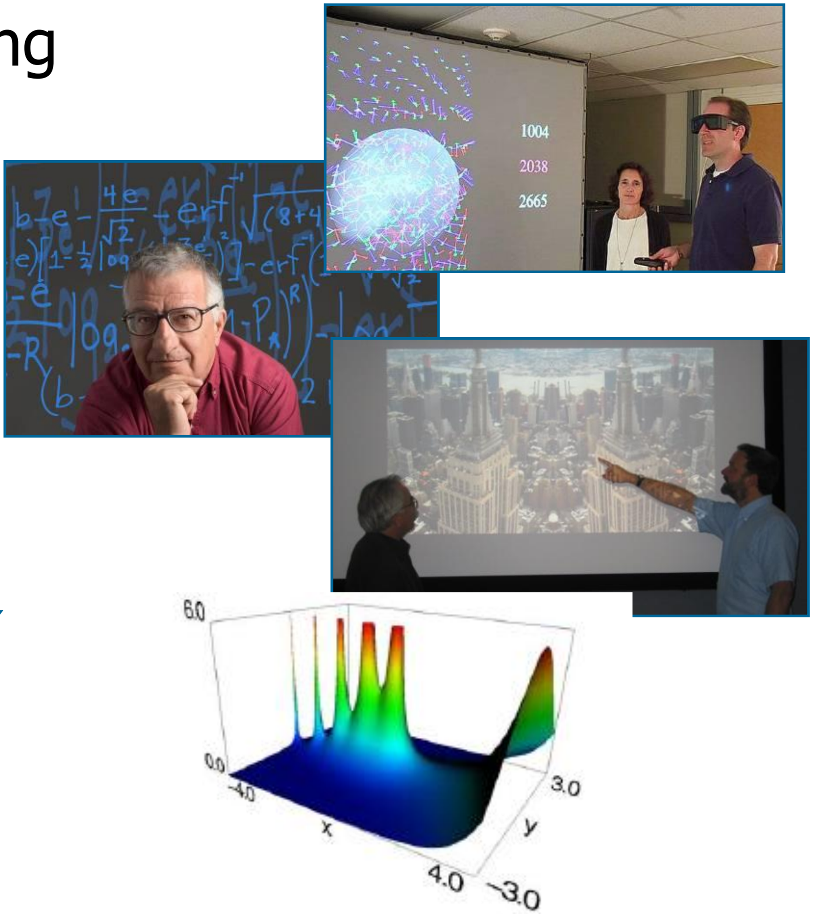
technology

through research and development in

information technology,

mathematics, and

statistics.



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

ITL Goals

- Accelerate the development and deployment of reliable, secure, usable, and interoperable information and communication systems.
- Catalyze the development of particular applications of national importance that have significant IT requirements.
- Enable world-class measurement and testing through innovations in mathematics, statistics, and computer science.

ITL and Rugged Software

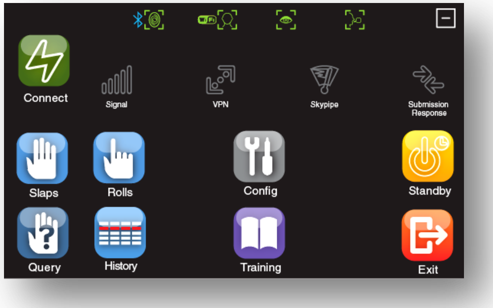
- “Rugged Software” is the theme of this Software Assurance Forum

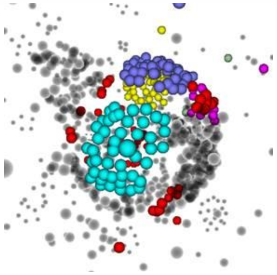
- NIST ITL provides guidance relevant to design, testing and deployment of software to meet critical national needs through NIST research, standards and guidance publications

NIST Addressing Critical National Needs

Examples:

- FISMA
- Software Assurance
- Secure Networking
- Enterprise Risk Management
- Usability
- Security Automation
- Foundations of Measurement Science for Information Systems





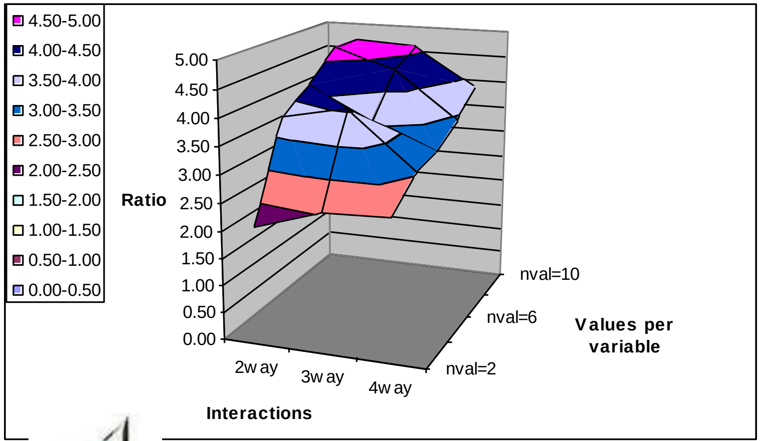
SAMATE

FISMA Support

- Supporting the implementation of and compliance with Federal Information Security Management Act (FISMA) through FIPS, Special Publications, and Guidelines, for example:
  - ***Security Categorizing of Federal Information and Information Systems*** by mission impact (FIPS 199).
  - ***Minimum Security Requirements for Federal Information and Information Systems*** (FIPS 200).
  - ***Recommended Security Controls for Federal Information Systems*** (SP 800-53 Rev 3).
  - ***Guide for Assessing the Security Controls in Federal Information Systems*** and determining security control effectiveness (SP 800-53A)
  - ***Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*** (SP 800-37 Revision 1).

Software Assurance

- Accelerate the development and adoption of correct, reliable, testable software, leading to increased trust and confidence in deployed software
  - Automated Combinatorial Testing for Software
  - Software Assurance Metrics
  - Static Analysis Tool Exposition
  - National Checklist Program

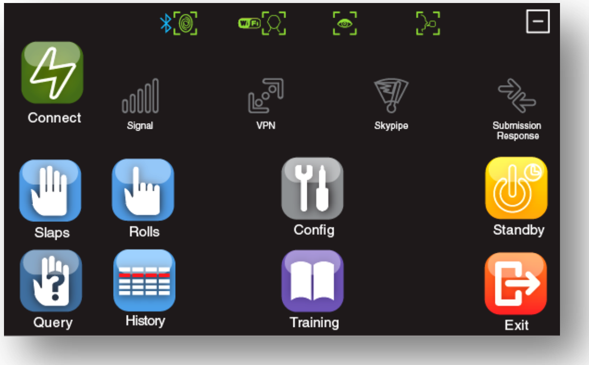


SAMATE

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

Usability

- User-centered research in human-system interaction by applying human factors scientific principles and methodologies to national priorities in the field of information technology
  - Usability Metrics & Measurements
  - Usability for Biometric Systems
  - Usability in Health IT
  - Usability and Accessibility of Voting Systems



Courtesy: Shutterstock/Brian A. Jackson

Security Automation

- NIST security standards and publications support automation in software security assurance.
  - ***SCAP: Security Content Automation Protocol*** (SP 800-126 Rev. 1) enables automated tooling for:
    - Vulnerability Management, Configuration Verification, Patch Compliance, System Inventory, Malware Detection.
  - ***Proposed Open Specifications for an Enterprise Remediation Automation Framework*** (Draft NISTIR 7670) The success of SCAP in automated system assessment has fostered research related to the development of similar open specifications in support of enterprise remediation use cases. A derived requirement to support this capability would be a "Common Remediation Enumeration" (CRE).

Secure Networking

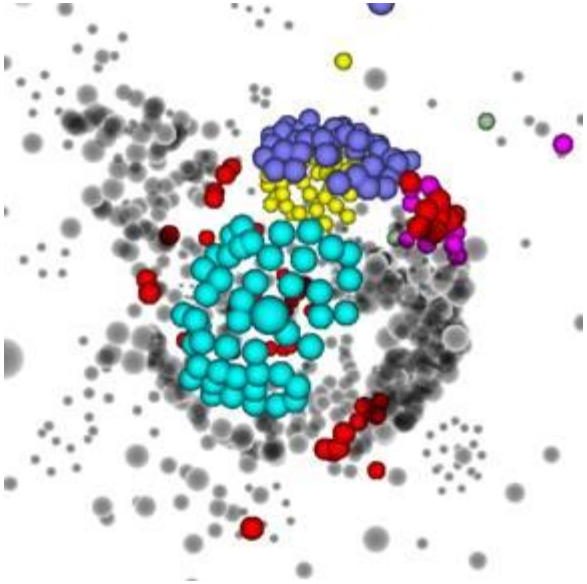
- ***Guidelines for the Secure Deployment of IPv6*** (SP 800-119) educates the reader about IPv6 features and the security impacts of those features. Provides a comprehensive survey of mechanisms that can be used for the deployment of IPv6. Provides a suggested deployment strategy for moving to an IPv6 environment.
- ***Guide to Bluetooth Security*** (SP 800-121) provides a background on Bluetooth technology characteristics, architecture and features. More importantly, it identifies types of vulnerabilities, threats, risk mitigation and countermeasures.
- ***Security Considerations for Voice Over IP Systems*** SP (800-58) is essential for any government agency using, or contemplating, Voice over IP. It is also highly recommended reading for any private organization using VoIP that is subject to IT security compliance audits.
- ***Multiple Special Publications on Wireless Network Security***
  - ***Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*** (SP 800-97)
  - ***Guide to Securing WiMAX Wireless Communications*** (SP 800-127).

Enterprise-Wide Risk Management

- ***Integrated Enterprise-Wide Risk Management: Organization, Mission and Information System View*** (SP 800-39) introduces a three-tiered risk management approach that allows organizations to focus, initially, on establishing an enterprise-wide risk management strategy as part of a mature governance structure involving senior leaders/executives and a robust risk executive (function).

Foundations of Measurement Science for Information Systems

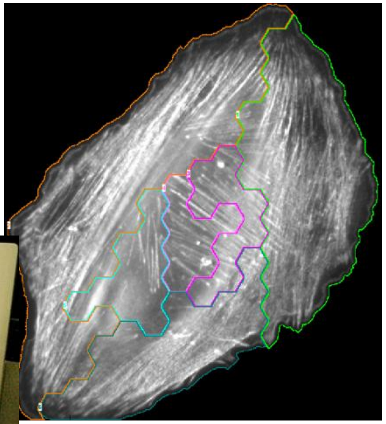
- Develop metrics for assessing critical properties of information systems that can be used to both design more reliable and secure systems, as well as to enable effective real-time control of deployed systems.
  - Macro-scale structure and dynamics of large-scale interconnected systems
  - Identify and characterize fundamental measurable properties of complex information systems that are indicators of the systems' inherent level of security and reliability
  - Complex Networks Data Sets



NIST Addressing Critical National Needs – Applications

Examples:

- Healthcare
- Cyber Security
- Smart Grid
- Cloud Computing
- Voting Systems
- Computer Forensics
- Identity Management



Other NIST Speakers

- Ernest McDuffie – Today – Panel Discussion on: "Identifying Synergies Between Software Assurance, Supply Chain Risk Management and Cyber Workforce Transformation" – will discuss the National Initiative in CyberSecurity Education (NICE).

- Ajit Jillavenkatesa – Wednesday – "Addressing Federal Agencies Engagement in Standards"

- Jon Boyens – Wednesday – Supply Chain – NISTIR 7622 – "Piloting Supply Chain Risk Management Practices for Federal Information Systems"

- Paul Black – Thursday – "Software Labeling"

- Mike Kass – Thursday – "Technology, Tools and Product Evaluation (TT&PE) Working Group Outbrief"

In Closing

- Standards are critical for ensuring interoperability, security, usability, and reliability (“ruggedness”) of software based systems.

- Testing requirements associated with standards need to be considered.

- Standards are best developed with broad participation – e.g., public/private partnerships – so get involved!

www.itl.nist.gov

BACKUP MATERIAL

NIST Addressing Critical National Needs
Healthcare

Standards for National Priority Critical Infrastructures: Health Information Technology

- Support progress toward a nationwide healthcare information infrastructure by
  - Developing and harmonizing usable standards for health IT technologies
  - Creating a health IT technology testing infrastructure

Biomedical Measurements to Support Disease Diagnosis and Treatment

- Develop the measurement science and reference materials to improve the accuracy, reproducibility, and efficacy of measurements used in medical diagnostics and imaging
- Develop the measurement science and standards to support manufacturing and regulatory approval of biologic drugs

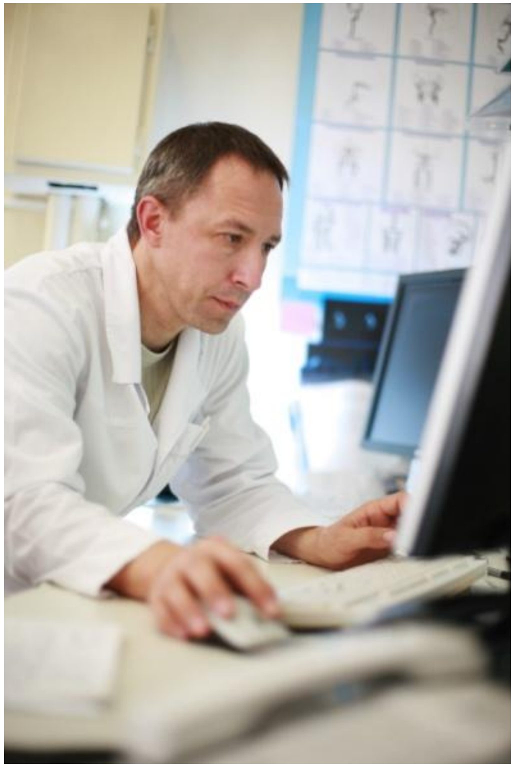
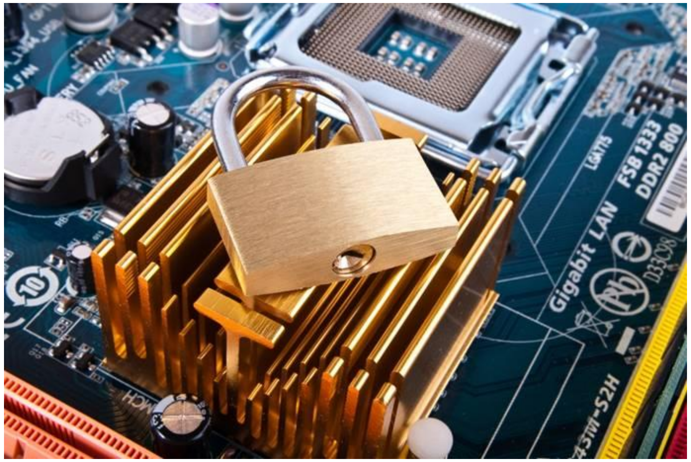


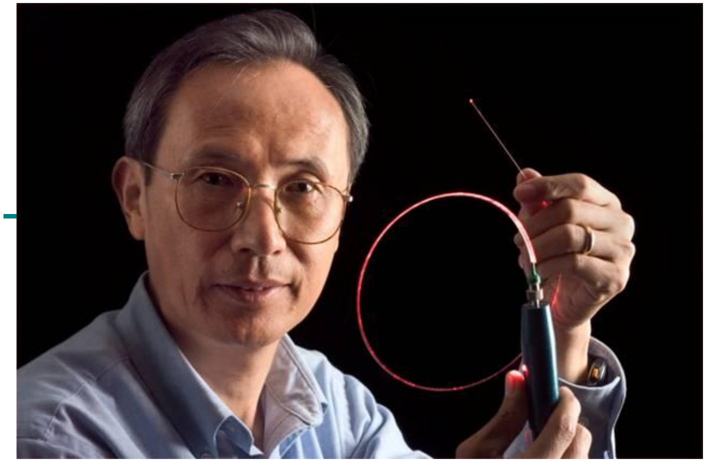
Image: Shutterstock, ©Konstantin Sutyagin

NIST addressing critical national needs – Cyber Security

- Scalable cybersecurity for emerging technologies and threats
  - Improved cryptographic capabilities
  - Stronger assurance of online user identities
  - Easier-to-use security mechanisms
  - Increased use of security automation technology
  - Security measurement for large-scale systems
  - Secure adoption of emerging virtual technologies
  - Critical infrastructure testbed development



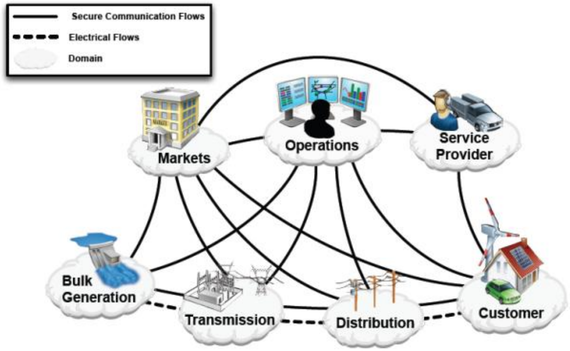
©Shutterstock/freebird



©Robert Rathe

NIST addressing critical national needs – Smart Grid Interoperability

- ***Guidelines for Smart Grid Cyber Security*** (NISTIR 7628) is:
  - A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies—established and emerging.
  - An evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation, and maintenance.
  - A guide to assist organizations as they craft a Smart Grid cyber security strategy that includes requirements to mitigate risks and privacy issues pertaining to Smart Grid customers and uses of their data.



NIST Smart Grid Framework 1.0 January 2010

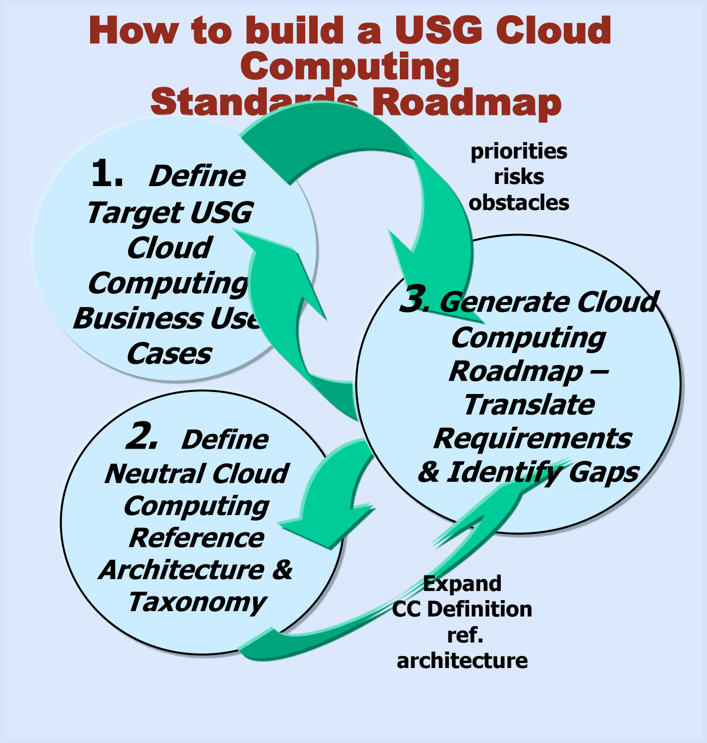
NIST Support of Cloud Computing

Strategic Initiave

- Goal: collaborate with Federal Chief Information Officers, Industry and Standards Developing Organizations to define a Cloud Computing Roadmap in support of the Federal CIO's "Cloud First" policy.
- The strategy was developed from May-Sept. 2010, and launched with stakeholders in November, 2010

Ongoing efforts

- Special Publications – recommendations and guidance
- Complex Information Systems Analysis
- Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)
- Technical Advisor to Federal CIO Council – Federal Risk & Authorization Management Program (FedRAMP)



How to build a USG Cloud Computing Standards Roadmap

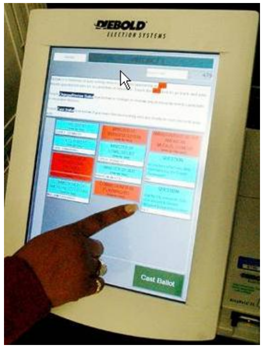
1. *Define Target USG Cloud Computing Business Use Cases*

2. *Define Neutral Cloud Computing Reference Architecture & Taxonomy*

3. *Generate Cloud Computing Roadmap – Translate Requirements & Identify Gaps*

NIST addressing critical national needs – Voting Systems

- Develop approaches, methods, algorithms, and prototype software tools for production of searchable math repositories with full semantics, and for upgrading existing math repositories to endow them with these same capabilities
  - Standards and Conformance Testing of Voting Systems
  - Usability and Accessibility of Voting Systems
  - Voting System Security

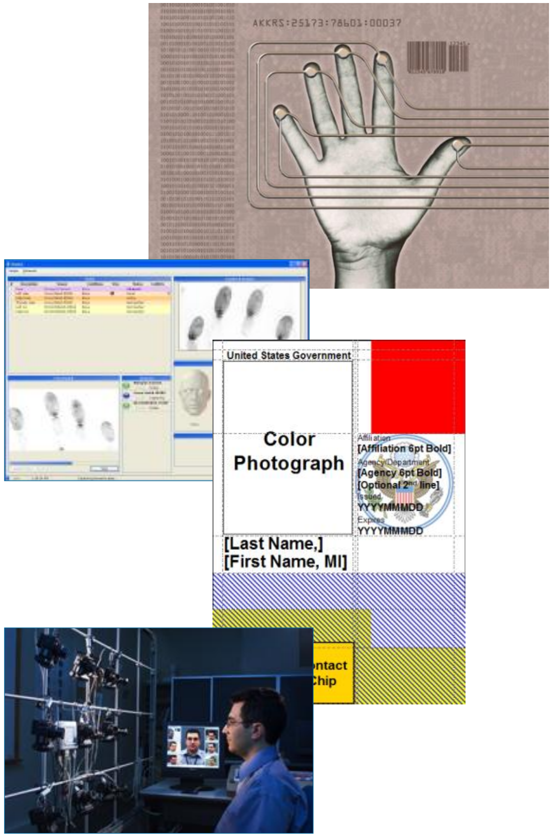


NIST addressing critical national needs – Computer Forensics

- Provide infrastructure necessary for automated processing in computer forensic investigations with scientific rigor necessary to support introduction of evidence
  - National Software Reference Library
  - Computer Forensics Tool Testing
  - Computer Forensics Tool Testing for Mobile Devices
  - Computer Forensics Reference Data Sets

NIST addressing critical national needs – Identity Management

- National Program Office for the National Strategy for Trusted Identities in Cyberspace (NSTIC).
- Advance Identity Management Systems technologies to ensure security, cost effectiveness and interoperability
  - Face & Iris Testing
  - Fingerprint Technology Testing for Identity Management
  - Identity Credential Interoperability
  - IDMS Research & Development
  - IDMS Standards Activities
  - Multimodal Biometrics
  - Research for Next Generation Biometric Measurements & Standards (NGBMS) for Identity Management
  - Usability of Biometric Systems

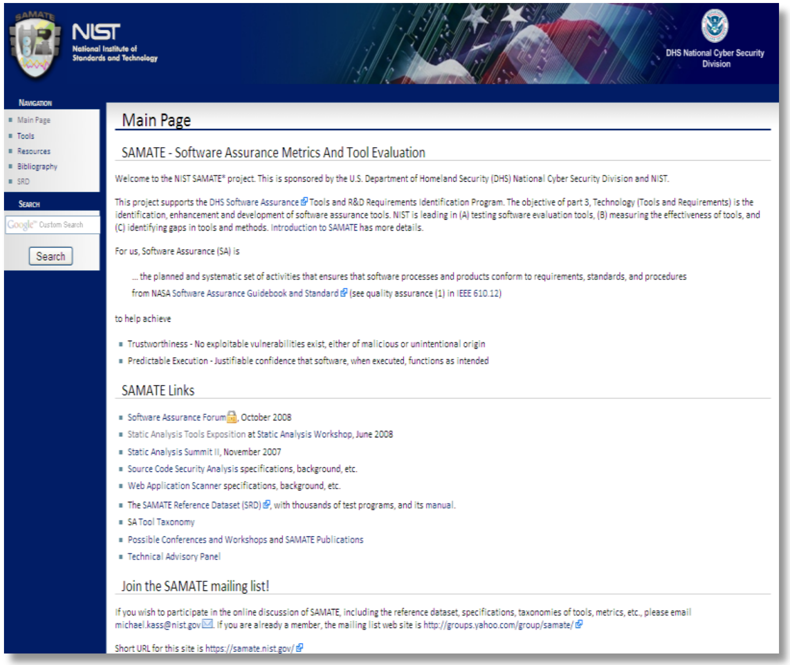


© Graeme Dawes | Dreamstime.com

Software Assurance Metrics and Tool Evaluation (SAMATE)

http://samate.nist.gov/

- NIST SAMATE co-sponsored with DHS to:
  - Measure of the effectiveness of today's software assurance tools
  - Identify gaps in technology
  - Recommend areas of research to DHS NCSD
  - Define metrics for the measurement of SwA tool effectiveness



Main Page

SAMATE - Software Assurance Metrics And Tool Evaluation

Welcome to the NIST SAMATE* project. This is sponsored by the U.S. Department of Homeland Security (DHS) National Cyber Security Division and NIST.

This project supports the DHS Software Assurance Tools and R&D Requirements Identification Program. The objective of part 3, Technology (Tools and Requirements) is the identification, enhancement and development of software assurance tools. NIST is leading in (A) testing software evaluation tools, (B) measuring the effectiveness of tools, and (C) identifying gaps in tools and methods. Introduction to SAMATE has more details.

For us, Software Assurance (SA) is

> ... the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures
>
> from NASA Software Assurance Guidebook and Standard (see quality assurance (1) in IEEE 610.12)

to help achieve

- Trustworthiness - No exploitable vulnerabilities exist, either of malicious or unintentional origin
- Predictable Execution - Justifiable confidence that software, when executed, functions as intended

SAMATE Links

- Software Assurance Forum, October 2008
- Static Analysis Tools Exposition at Static Analysis Workshop, June 2008
- Static Analysis Summit II, November 2007
- Source Code Security Analysis specifications, background, etc.
- Web Application Scanner specifications, background, etc.
- The SAMATE Reference Dataset (SRD), with thousands of test programs, and its manual.
- SA Tool Taxonomy
- Possible Conferences and Workshops and SAMATE Publications
- Technical Advisory Panel

Join the SAMATE mailing list!

If you wish to participate in the online discussion of SAMATE, including the reference dataset, specifications, taxonomies of tools, metrics, etc., please email michael.kass@nist.gov. If you are already a member, the mailing list web site is http://groups.yahoo.com/group/samate/

Short URL for this site is https://samate.nist.gov/

Static Analysis Tool Exposition (SATE)

- Static Analysis Tool Exposition (SATE) is designed to advance research (based on large test sets) in, and improvement of, static analysis tools that find security-relevant defects in source code.

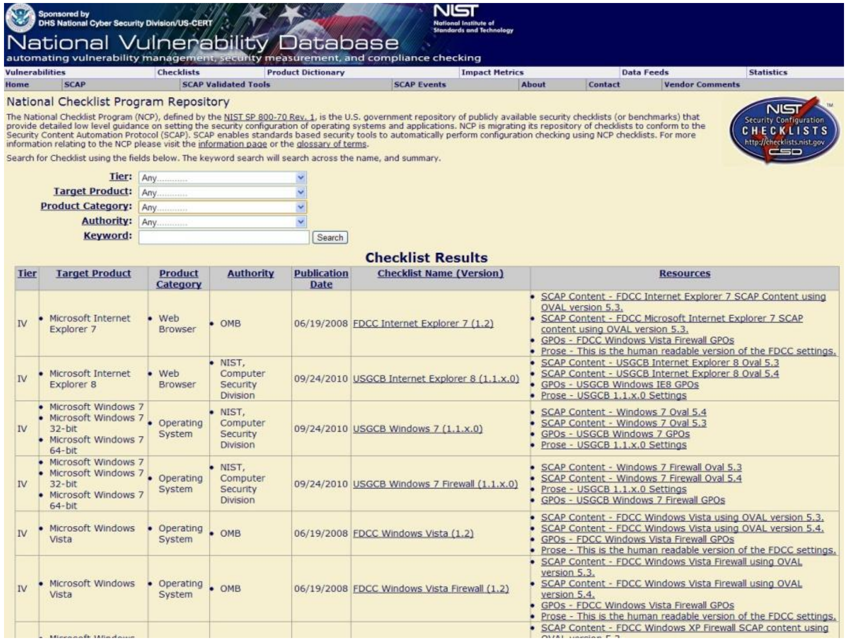
- Participating tool makers run their tools on a set of programs. Researchers led by NIST analyze the tool reports. The results and experiences are reported at a workshop. The tool reports and analysis are made publicly available later.

  - The goals of SATE are:
    - To encourage improvement of tools
    - To speed adoption of tools by objectively demonstrating their use on real software
    - Enable empirical research based on large test sets

National Checklist Program (NCP)

http://web.nvd.nist.gov/view/ncp/repository

- The National Checklist Program is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.
- NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP).



Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 1, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: Any............
Target Product: Any............
Product Category: Any............
Authority: Any............
Keyword:
Search

Checklist Results

Tier	Target Product	Product Category	Authority	Publication Date	Checklist Name (Version)	Resources
IV	• Microsoft Internet Explorer 7	• Web Browser	• OMB	06/19/2008	FDCC Internet Explorer 7 (1.2)	• SCAP Content - FDCC Internet Explorer 7 SCAP Content using OVAL version 5.3. • SCAP Content - FDCC Microsoft Internet Explorer 7 SCAP content using OVAL version 5.3. • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings.
IV	• Microsoft Internet Explorer 8	• Web Browser	• NIST, Computer Security Division	09/24/2010	USGCB Internet Explorer 8 (1.1.x.0)	• SCAP Content - USGCB Internet Explorer 8 Oval 5.3 • SCAP Content - USGCB Internet Explorer 8 Oval 5.4 • GPOs - USGCB Windows IE8 GPOs • Prose - USGCB 1.1.x.0 Settings
IV	• Microsoft Windows 7 • Microsoft Windows 7 32-bit • Microsoft Windows 7 64-bit	• Operating System	• NIST, Computer Security Division	09/24/2010	USGCB Windows 7 (1.1.x.0)	• SCAP Content - Windows 7 Oval 5.4 • SCAP Content - Windows 7 Oval 5.3 • GPOs - USGCB Windows 7 GPOs • Prose - USGCB 1.1.x.0 Settings
IV	• Microsoft Windows 7 • Microsoft Windows 7 32-bit • Microsoft Windows 7 64-bit	• Operating System	• NIST, Computer Security Division	09/24/2010	USGCB Windows 7 Firewall (1.1.x.0)	• SCAP Content - Windows 7 Firewall Oval 5.3 • SCAP Content - Windows 7 Firewall Oval 5.4 • Prose - USGCB 1.1.x.0 Settings • GPOs - USGCB Windows 7 Firewall GPOs
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista (1.2)	• SCAP Content - FDCC Windows Vista using OVAL version 5.3. • SCAP Content - FDCC Windows Vista using OVAL version 5.4. • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings.
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista Firewall (1.2)	• SCAP Content - FDCC Windows Vista Firewall using OVAL version 5.3. • SCAP Content - FDCC Windows Vista Firewall using OVAL version 5.4. • GPOs - FDCC Windows Vista Firewall GPOs • Prose - This is the human readable version of the FDCC settings.
	• Microsoft Windows					• SCAP Content - FDCC Windows XP Firewall SCAP content using

Homeland Security

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

Advanced Combinatorial Testing

- Software developers frequently encounter failures that result from an interaction between components. Testers often use pairwise testing – all pairs of parameter values – to detect such interactions
- Combinatorial testing beyond pairwise is rarely used because good algorithms for higher strength combinations (e.g., 4-way or more) have not been available
- NIST is producing methods and tools to generate tests for all *n*-way combinations of parameter values, using improved combinatorial testing algorithms for constructing covering arrays, and automated generation of test oracles.