



# *Information Technology Laboratory Technical Accomplishments*

# 2003



Building Trust and Confidence  
in IT through Standards,  
Measurements, and Technology

NISTIR 7034



**National Institute of Standards and Technology**  
Technology Administration, U.S. Department of Commerce

NISTIR 7034  
DECEMBER 2003



## **U.S. DEPARTMENT OF COMMERCE**

Donald L. Evans, Secretary

### **Technology Administration**

Phillip J. Bond

Under Secretary of Commerce for Technology

National Institute of

Standards and Technology

Arden L. Bement, Jr., Director

---

### **About ITL**

*For more information about ITL, contact:*

Information Technology Laboratory  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 8900  
Gaithersburg, MD 20899-8900

Telephone: (301) 975-2900

Facsimile: (301) 840-1357

E-mail: [itlab@nist.gov](mailto:itlab@nist.gov)

Web site: <http://www.itl.nist.gov>

## **C O N T E N T S**

|  |    |
|--|----|
| Director's Foreword                        | 1  |
| ITL at a Glance                            | 4  |
| ITL Research Blueprint                     | 6  |
| Accomplishments of our<br>Research Program | 7  |
| Foundation Research Areas                  | 8  |
| Selected Cross -Cutting Themes             | 29 |
| Industry and International Interactions    | 35 |
| Staff Recognition                          | 42 |

# DIRECTOR'S FOREWORD

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) is pleased to present its accomplishments for 2003. Our mission is to develop and promote measurement science, standards, and supporting programs in information technology (IT) in order to enhance productivity, facilitate trade, and improve the quality of life. We work in partnership with industry, academia, government, and consortia to develop and demonstrate tests, test methods, reference data, proof-of-concept implementations, and other IT infrastructure technologies. Our goal is to enable the IT industry in the United States to produce products and services that are of high quality, and that are reliable, interoperable, and secure.

In 2003, ITL continued its work under a growing number of legislative mandates in areas ranging from cyber security research and development to voting standards and guidelines. The Cyber Security Research and Development Act assigns key cyber security responsibilities to NIST including, among others, intramural research in multidisciplinary, long-term, high-risk cyber security areas. The Federal Information Security Management Act assigns NIST the responsibility to develop cyber security standards, guidelines, and associated methods and techniques. The USA PATRIOT Act requires NIST to develop and certify a technology standard, including appropriate biometric identifier standards, that can be used by federal agencies to verify the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa. The Help America Vote Act requires NIST to provide technical support to the newly formed Election Assistance Commission through research and development to support the development of voluntary



*Susan F. Zevin,  
Acting ITL Director*

voting system guidelines. The combination of our mission and mandates leads to a rich programmatic diversity.

The ITL program has been rich with accomplishments in the past, including leading the worldwide competition for the Advanced Encryption Standard, developing and implementing the XML Test Suite in the World Wide Web, developing a Braille Reader, writing the popular NIST/Sematech e-Handbook of Statistical Methods, developing a JAVA Numerics language for the scientific community, developing the widely known and used Common Industry Format for Usability Test Reports, and establishing the National Software Reference Library and Computer Forensics Toolkit in support of the nation's law enforcement community. The results of many of these efforts can be viewed on the ITL website at <http://www.itl.nist.gov>.

This year we have initiated new efforts, expanded some nascent efforts, and furthered key programs in response to our customer's needs, thereby ensuring that we provide the best value to the United States. We present the details in the following pages. Here are highlights from our major program areas:

**Security.** The contributions to the nation from our security program continue to grow through its comprehensive cryptographic toolkit; expanded technical guidelines and standards publications with particular emphasis on certification and accreditation, access controls, categorization of security systems, and development of minimum security requirements for systems; assistance to federal agencies and industry through computer security management guidelines; and services based on sound testing methodologies and test metrics.

**Software.** ITL maintains a robust program in software that is fundamental to the continued growth of the IT industry. In FY 2003, the software program facilitated electronic commerce through development of XML tests; developed test methods and registries to improve the interoperability, quality, conformance, and correctness of healthcare standards; reduced computer forensic investigation time by as much as 85 percent with the latest release of the National Software Reference Library; developed measurements to ensure that service discovery protocols can perform under volatile conditions; and utilized automatic test generation to improve the interoperability of smart cards.

**Networks.** Our networking group has made significant progress in measurement and evaluation programs that are key in the implementation, robust operation, and continuity of operations of the nation's core networking infrastructure. In FY 2003, the networking program continued to validate, simulate, and analyze wireless personal area network protocols; developed service discovery protocols that allow devices to discover and invoke desired services; evaluated and developed protection and restoration methods through

agile switching infrastructures and network management; designed and evaluated technologies to expand the capability and scope of emerging Internet telephony signaling standards; and developed and deployed standardized Internet infrastructure protection technologies such as Domain Name System Security and large-scale virtual private network modeling and analysis.

**Information Access.** ITL continues to make strides in improving our customers' ability to utilize information. In FY 2003, the program evaluated advanced speech technologies that enabled a dramatic breakthrough in speech to text broadcast news error rates; worked with industry to develop MPEG and JPEG multimedia technologies and standards; provided metrics, standards, and test methodologies to improve the usability of interactive systems; and advanced smart space technologies through provision of a modular testbed for integration, interoperability, architecture development, data collection, and performance of experiments.

**Information Integration.** ITL continued efforts in the convergence of hardware and software. In FY 2003, the convergent information program focused on the preservation of digital media through media longevity studies; interoperability studies and development of guidelines and standards for archival storage media, systems, and networks; and development of a new refreshable tactile graphic display technology for the blind and visually impaired.

**Mathematics.** Our mathematics program provides technical leadership in state-of-the-art analytical and computational methods. In FY 2003, the mathematics program developed, analyzed, and solved mathematical models of physical phenomena; developed highly efficient parallel computational models to enable scientific advancement; developed and distributed mathematical software tools and tests, including the micromagnetic modeling software that helped to enable one of the top ten physics advances in 2002; and continued development of the Digital Library of



Mathematical Functions, a comprehensive, authoritative web-based interactive reference on the special functions of applied mathematics.

**Statistics.** ITL continues to provide the statistical underpinnings that strengthen scientific research through formulation and development of statistical theory and methodology for metrology. In FY 2003, the statistics program developed new Bayesian methods for metrology, expert elicitation for uncertainties, models, and designs, and Bayesian software and software testing; developed new statistical methods for the design and analysis of Key Comparisons which form the basis of international trade; developed statistical methods to evaluate IT performance in networks, biometrics, and computer forensics; characterized complex instruments, systems, and processes in mathematical terms, including the analysis of the World Trade Center collapse; and created a portable CD version of the popular NIST/Sematech e-Handbook of Statistical Methods.

ITL also focuses on several programs that merit treatment outside the bounds of each technical specialty due to their cross-disciplinary nature. In FY 2003, the voting program joined biometrics, critical infrastructure protection, healthcare, and quantum as one of these programs. The voting program was initiated this year to enhance the capacity and performance of the nation's voting systems through the development and promotion of standards, measures, and technologies. In FY 2003 the biometrics program centered on fingerprint and face recognition testing, multimodal biometrics evaluation and system design, and biometrics standards. The biometrics program released two key reports on the use of biometrics indicating the needs in homeland security and the state of the art: "Both Fingerprints, Facial Recognition Needed to Protect U.S. Borders" and "Significant Advances Made in Facial Recognition Technology in the Past Two Years." We continued to develop security standards, guidance, metrics, and testing programs to help protect our nation's critical infrastructures. Our healthcare program tackled the large problems in healthcare including efforts to increase quality

healthcare through enhancement of conformance, to develop registries and a healthcare standards roadmap, and sought answers to the critical impediments to widespread standardized electronic health record deployment. The quantum program saw major success in FY 2003 consisting of the development of a testbed for the distribution of cryptographic keys using a quantum channel, development and analysis of improved protocols for quantum key distribution, and development of architectural concepts for the design of quantum computers and the implementation of quantum algorithms.

Thank you for your interest in the Information Technology Laboratory. Please take a few minutes to review this document and learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology.

*Susan F. Zevin, Acting ITL Director  
Information Technology Laboratory  
E-mail: [itlab@nist.gov](mailto:itlab@nist.gov)*

# ITL AT A GLANCE



*Kamie Roberts*  
*Acting ITL*  
*Deputy Director*

## OUR MANAGEMENT TEAM

**Susan F. Zevin**, *Acting ITL Director, ITL Deputy Director*

**Kamie Roberts**, *Acting ITL Deputy Director, Associate Director for Federal and Industrial Relations*

**Bradley Alpert**, *Acting Assistant Director for Boulder*

**Kendra Cole**, *Senior Management Advisor*

**Ronald Boisvert**, *Chief of Mathematical and Computational Sciences Division*

**David Su**, *Chief of Advanced Network Technologies Division*

**Edward Roback**, *Chief of Computer Security Division*

**Martin Herman**, *Chief of Information Access Division*

**Gordon Lyon**, *Acting Chief of Convergent Information Systems Division*

**Mark Skall**, *Chief of Software Diagnostics and Conformance Testing Division*

**Nell Sedransk**, *Chief of Statistical Engineering Division*

## OUR CORE PURPOSE

Enabling a better future through information technology (IT).

## OUR MISSION

To develop and promote measurement, standards, and technology for information technology to enhance productivity, facilitate trade, and improve the quality of life. We also help federal agencies in understanding and arranging for computer security.

## OUR VISION

To be the global leader in measurement and enabling technology for information technology, delivering outstanding value to the nation.

## OUR RESOURCES

- highly qualified professional and support staff of 331 (includes part-time, students, and faculty appointments), supplemented by 151 guest researchers (as of September 20, 2003)
- total authorization for fiscal year 2003 budget of \$70.2M, all sources (as of September 20, 2003)
- research and operations facilities in Gaithersburg, Maryland, and Boulder, Colorado
- opportunities for cooperative research and interaction with industry and academia

## OUR PRODUCTS AND SERVICES

- reference data sets and evaluation software
- tests and test methods
- standards
- proof-of-concept implementations
- advanced software tools
- automated software testing techniques
- statistical model-based testing
- specialized databases
- electronic information on the web
- mathematical and statistical consulting services

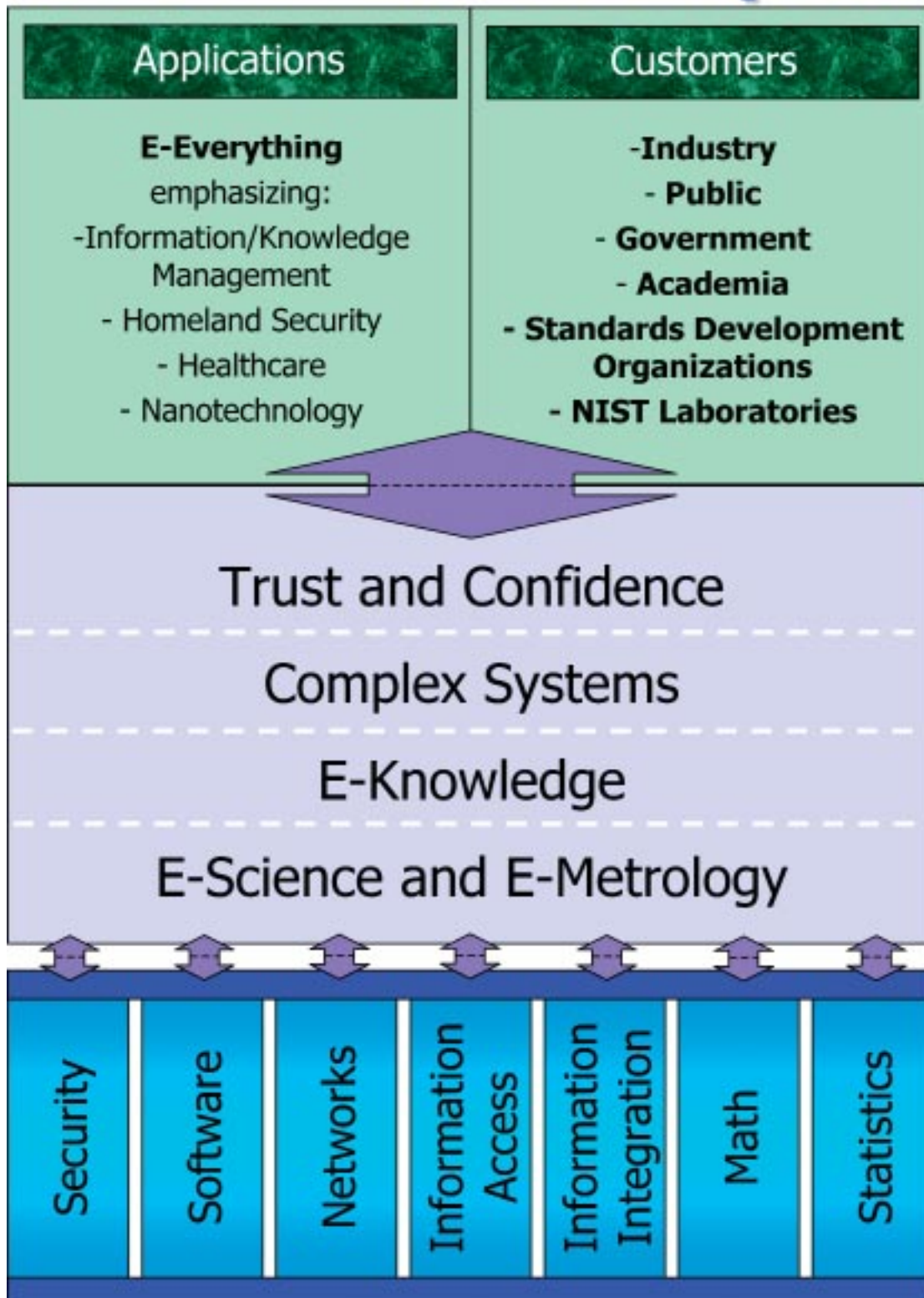
## OUR CUSTOMERS

- U.S. industry
- federal agencies
- academia
- NIST staff and collaborators
- research laboratories
- IT users and providers
- industry standards organizations

## OUR RESEARCH PROGRAM

The following chart presents the ITL Research Blueprint, the framework by which we describe our research program. The seven core research areas at the base establish a solid foundation in IT standards, measurements, and technology. These areas form the basis of ITL's efforts in four thematic areas, such as building trust and confidence in IT systems. This research approach provides enabling technologies necessary to achieve the promise of E-Everything for our customers.

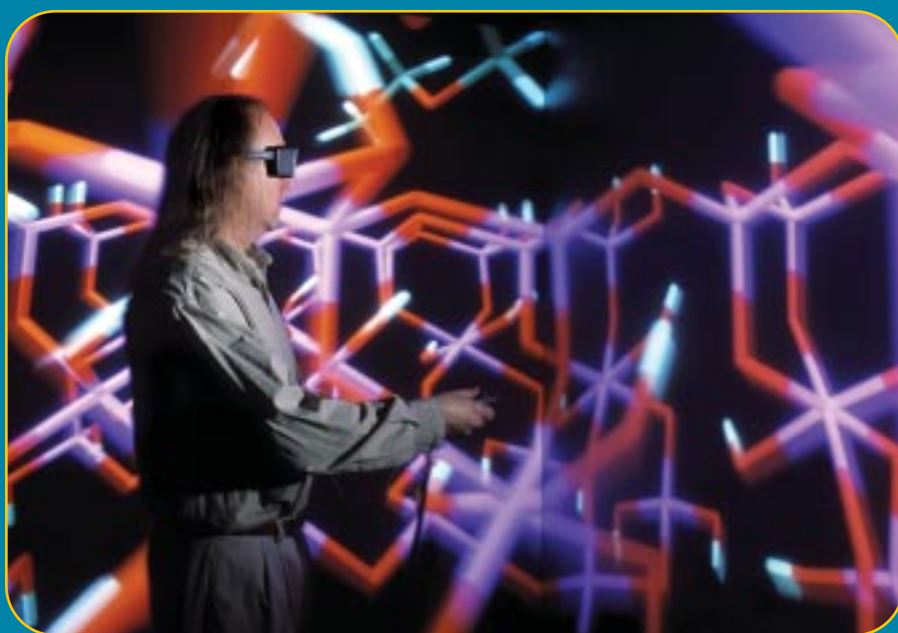
# ITL Research Blueprint





# ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

---



© Robert Rathe

*ITL Computer Scientist Steve Satterfield examines his visualization of a smart gel in an immersive environment. This was joint work with Carlos Gonzalez (not pictured) of NIST's Chemical Science and Technology Laboratory.*

## FOUNDATION RESEARCH AREAS

## SECURITY



*Jim Dray and Teresa Schwarzhoff discuss the smart card interoperability specification, which will help improve security of federal sites and systems.*

## SECURITY TECHNOLOGY

**ITL** is developing a comprehensive cryptographic toolkit that will enable federal agencies and others to select cryptographic security components and functionality for protecting their data, communications, and operations. The toolkit currently includes a wide variety of cryptographic algorithms and techniques for protecting the integrity, confidentiality, and authenticity of information resources, and helps enable the widespread implementation of cryptographic services in applications and the national infrastructure. Program areas include cryptographic standards, key management, public key infrastructure (PKI), identity management (IM), protocols and e-government, and agency e-government support. Our customers include federal agencies, industry,

state/local governments, researchers, testing laboratories, and IT users. The website is <http://csrc.nist.gov/CryptoToolkit/index.html>.

Our accomplishments in FY 2003 include many significant draft documents, standards, and validation tests. We wrote draft key management scheme and guideline documents, as well as the draft of a symmetric key management publication. We completed a recommendation on authentication modes of operation. We produced a draft Advanced Encryption Standard (AES) key wrap publication. We developed validation tests for authentication, the Digital Signature Algorithm, the Secure Hash Algorithm, the Keyed-Hash Message Authentication Code, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm. We produced a draft of a random

number generator standard (ANSI X9.82). We made available basic X.509 certification path validation tests. Lastly, we made available a draft Secure/Multipurpose Internet Mail Extensions (S/MIME) client profile, a draft S/MIME client protection profile (functionality and security), and a draft Transport Layer Security client and server protection profiles (functionality and security).

Our work in cryptography is making an impact within and outside the federal government. Strong cryptography is now used in commercial, off-the-shelf IT products. Strong PKI and cryptography improve the security of systems and the information they process. IT users also enjoy the enhanced availability in the marketplace of secure applications through cryptography and PKI. See <http://csrc.nist.gov/pki>.

## SYSTEMS AND NETWORK SECURITY

ITL continued its robust technical program to protect information systems and the networks that connect them. Our technical guidelines and standards, publications, *ITL Bulletins*, checklists, online resources, and specifications address a wide range of critical areas, including smart cards, wireless/mobile computing, intrusion detection systems (IDSs), vulnerabilities, Internet protocol security (IPsec), and authorization management. Federal agencies rely on the NIST technical guidelines, which are frequently cited and reused by industry on a voluntary basis.

In FY2003, we published technical guidance on smart cards, incident handling, voice over Internet Protocol, procurement, products and services, network security testing, IDS testing, and security metrics. Nine *ITL Bulletins* were published; these are widely read inside and outside of the federal government. We completed a Windows 2000 baseline and guideline to protect the Windows 2000 Professional system from common vulnerabilities. NIST published the Government Smart Card Interoperability Specification (GSC-IS), version 2.1, which helps to reduce the cost of smart card integration. The online ICAT vulnerability database was enhanced and now contains about 6,000 entries. ICAT enables system administrators to identify flawed systems and to find the patches. A PKI interaction was added to our IPsec-WIT Interoperability Tester, which has been used by over 225 organizations. We proposed our Role Based Access Control (RBAC) work as a national voluntary standard and published a book on RBAC. Websites are <http://csrc.nist.gov/publications/>, <http://icat.nist.gov/icat.cfm>, and <http://csrc.nist.gov/rbac/>.

## MANAGEMENT AND ASSISTANCE

A significant component of our computer security program is our outreach, expert assistance, policy, and guidelines for federal agencies, industry, and small and medium-size businesses. Our efforts result in increased effectiveness of federal agency computer security programs and improved cost-effectiveness for agencies

by eliminating duplication of effort. By fostering the use of shared security practices among federal agencies, ITL enables agencies to plan and budget appropriately for computer security, address their policy and management needs, and meet legislated computer security requirements. We direct our new guidelines development efforts where they are most needed, in areas identified by such advisory groups as the Information Security and Privacy Advisory Board, which we support. We also host the Federal Computer Security Program Manager's Forum quarterly meetings to provide insight to and receive feedback from the federal community.

In FY 2003, we developed several significant new guidance documents, including a security metrics guideline, procurement guidance for security, and a contingency planning guide. We initiated a capital planning guideline initiative and conducted two NIST/OMB capital planning workshops. We participated in several critical federal workgroups dealing with procurement security issues. We enhanced our ASSET software for agencies to perform security self-assessments. Based on agency feedback, we revised our Computer Security Expert Assist Team (CSEAT)



*Joan Hash and Patrick O'Reilly discuss the continual growth and evolution of the Computer Security Resource Center <http://csrc.nist.gov>. The CSRC is one of the most visited NIST websites.*



*Murugiah Souppaya and John Wack discuss the development of security checklists for widely used IT products.*

methodology to better serve federal agencies that request security program reviews. We also improved and maintained our Computer Security Resource Center (CSRC), one of the most visited websites at NIST: <http://csrc.nist.gov>.

Our support of small- and medium-sized businesses continued. We added a small business corner to our CSRC website. We grew community college and Small Business Development Corporation participation to the national level, making NIST a viable information security resource for existing, localized, small business support infrastructure. We also launched a NIST Small Business Administration InfraGard Small Business Resource Group. The website is <http://sbc.nist.gov/>.

## SECURITY TESTING AND METRICS

The goal of our security testing and metrics program is to provide our customers with a proven set of IT security services based on sound testing methodologies and test metrics. Program components include the Cryptographic Module Validation Program (CMVP), testing laboratory accreditation, the National Information Assurance Partnership (NIAP), and certification and accreditation.

The CMVP provides federal agencies in the United States and Canada with confidence that a validated cryptographic product correctly implements government cryptographic standards. As of September 30, 2003, the CMVP had issued 348 validation certificates representing 775 individual cryptographic modules from 99 IT vendors. We expanded the reach of the CMVP to include the United Kingdom and added an accredited testing laboratory in that country, for a total of seven laboratories. The website is <http://csrc.nist.gov/cryptval>. We initiated work in the International Organization for Standardization for the international adoption of Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. We supported a national level review of NIAP called for by the White House in the *National Strategy to Secure Cyberspace*. In response to a mandate under the Federal Information Security Management Act of 2002, we produced a draft FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, as well as a draft *Guide for the Security Certification and Accreditation of Federal Information Systems*. We also initiated development of a draft *Minimum Recommended Security Controls for Information Systems* guideline and initiated the draft of a companion validation document.

The impact of ITL's information security program is significant, notable in the increased security of IT systems through the availability of tested products. Our program also creates business opportunities for vendors of security products, testing laboratories, and security consultants.



## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

## SOFTWARE

## ELECTRONIC COMMERCE

To facilitate electronic commerce, ITL is developing software testing tools and methods that improve quality, conformance to standards, and correctness. Projects include XML Core (XML, XInclude, Namespace), Document Object Model (DOM) (L1, L2, HTML), XSL-FO, XSLT, Schema (data types, list/union, constraints, validation rules), and XQuery (functions and operators). We lead the conformance testing efforts for all of these projects. We initiated an effort to consolidate our testing methods into an automated method for generating tests based on XML technologies. In FY 2003, we completed and released new tests for Namespace, Schema, and XQuery. With the World Wide Web Consortium (W3C), we jointly issued public releases for XInclude and DOM 1.2 HTML test suites. We completed an XSL-FO test suite with more than 2,100 tests. We presented a paper on Schema testing at the XML 2003 Conference. Lastly, we completed our DOM, XSL-FO, and XSLT projects; we developed 25,000 total tests during the life of these projects, including 6,000 in FY 2003.

We continued our W3C conformance advisory role. We co-chair the W3C Quality Assurance (QA) Interest Group and participate in the QA Working Group (WG). We serve as editors and major contributors to the QA Guidelines; the W3C WGs are using the QA Guidelines to improve their charters, operational processes, and specifications. We developed QA Process documents for XML, DOM, and Schema. Our expertise contributes to higher-quality specifications and test suites.

A related project is the development of a consistent test framework for electronic business XML (ebXML). Working with the Organization for the Advancement of Structured Information Standards (OASIS), we advanced our Standards Registries and Messaging project in



*Eric Dalci, Elizabeth Fong, and Alan Goldfine develop conformance tests for smart cards.*

FY 2003. We developed conformance test suites for the ebXML Registry specifications, which verify open source ebXML. We completed our Registry project and transferred the technology to industry. Messaging allows for the exchange of ebXML transactions and registries. For the Messaging specification, we lead the conformance effort in OASIS and developed the ebXML Test Framework Specification v1.0, which was approved as an OASIS Committee Specification. We also developed an initial Messaging test suite. Another area of interest is our smart card testing, including basic services interface (BSI) testing, card edge testing, and the Government Smart Card (GSC) test program. We improved the BSI specification and added a Java binding, rewrote the card edge specification and developed a test strategy, and delivered an operational testing plan for the GSC.

The impact of our conformance testing program is significant. Many software developers use our test suites, resulting in bug fixes to XML implementations and specifications. The test methodologies that we develop influence others, including Open Source Linux, OASIS, SourceForge, Apache, and the Government Smart Card-Interoperability Specification (GSC-IS). Our XML Tester Tool has been adopted by industry. ITL conformance tests continue to influence all XML software solutions, which are used by millions of consumers. The website is <http://www.nist.gov/xml>.

## E - HEALTH

In partnership with the healthcare industry, government agencies, and academia, ITL seeks to improve the quality of healthcare, reduce costs, and provide essential services through the use of information technology. Working closely with the Health Level 7 (HL7) Consortium, we focus on HL7 conformance, HL7 registry, and the healthcare standards roadmap. In FY 2003, we developed HL7 V2/V3 conformance definitions; the HL7 specifications were changed to support conformance. The HL7 Experimental Registry (Beta) was made available; this registry is integral to the

success of HL7 V3. We actively participate in the ANSI Health Informatics Standards Board, eGOV Consolidated Health Informatics, and Connecting for Health. We co-sponsored a telehealth workshop, with a focus on diabetic retinopathy standards. We also developed a healthcare standards roadmap metadata, schema, and initial prototype. ITL is now recognized as a major player in the healthcare arena.

We continued our work in healthcare information systems. For the Department of Veterans Affairs (VA), we successfully deployed the Enterprise Single Sign-On (ESSO) to all VA hospitals. We demonstrated and documented key principles for integrating ESSO into new system architectures with enhanced security. We created a testbed to build prototypes of emerging VA system architectures. Our efforts resulted in improved quality of the VA health information systems. See <http://www.nist.gov/ehealth>.

## COMPUTER FORENSICS

Sound computer forensics practices are key to finding and delivering court-admissible evidence when computers are used in the commission of a crime. Our computer forensics program consists of the National Software Reference Library (NSRL) and the Computer Forensics Tool Testing (CFTT) project. Both projects are coordinated by the NIST Office of Law Enforcement Standards and supported by the National Institute of Justice.

The NSRL is a reference data set of file signatures (hashes) of commercial, off-the-shelf (COTS) files, which can be used during examination of digital evidence to identify pertinent files and eliminate others. The NSRL data set can eliminate 40-95 percent of COTS files from examination and save hundreds of staff-hours. In FY 2003, we continued to update and populate the NSRL, which now contains over 17 million file signatures and 4,300 products from 480 vendors. In response to a request from federal investigators, we added 500 thousand Arabic files to the data set last year. The NSRL was also applied to presidential records.



*The HL7 (Health Level 7) Registry TEAM, Leonard Gallagher, John Barkley, William Majurski, Lisa Carnahan, Andrew McCaffrey, and Mary Laamanen (not pictured), help to improve conformance to healthcare message transactions.*

Our CFTT project provides a measure of assurance that the tools used in computer forensics investigations produce accurate results. We developed a specification, test methodology, and test software for disk imaging. We delivered test reports to the National Institute of Justice, including dd/Redhat, Safeback 2.0, Safeback 2.18, EnCase, and dd/FreeBSD. We also completed a specification and test software for write-blocking. Our NSRL and CFTT projects have been used in terrorist investigations, including the Moussaoui case and thousands of law enforcement cases. Both projects have received international recognition. The websites are <http://www.nsrl.nist.gov/> and <http://www.cftt.nist.gov/>.

## SERVICE DISCOVERY PROTOCOLS

Current trends show that software systems comprise collections of components that combine and recombine dynamically in reaction to changing conditions. Service discovery protocols (SDPs) enable software components to locate available software services and adapt to changing topology. This project uses architectural system modeling to improve the quality and robustness of SDPs in distributed systems and develop system performance measurements. In FY 2003, we developed consistency conditions as the basis for measurements. We developed a Unified Modeling Language (UML) model of an abstract SDP, providing industry with a comparison tool. We developed generic test scenarios, performed experiments, and reported results at four workshops and conferences. Our work contributed to the improvement of SDP specifications. We also provided needed metrics for the performance of dynamic systems. In FY 2003, we applied our knowledge of SDP behavior to self-healing systems. In particular, we initiated a new effort to improve the quality and reliability of service for Grid Computing systems. The website is [http://www.itl.nist.gov/div897/docs/adl\\_servicediscovery.html](http://www.itl.nist.gov/div897/docs/adl_servicediscovery.html).

## TEST METHOD RESEARCH

To improve the development of specifications, software tests, and software quality, ITL develops tools and techniques to automate the labor-intensive process of software testing. Our automated test generation (ATG)



*Leonard Gallagher, Jeff Offutt, Julie Zanon, and Anthony Cincotta develop new test methods for object-oriented software.*

provides a method for automatically generating tests from formal specifications. This involves the development, validation, and application of a model. In FY 2003, we created a formal specification, developed the test environment, and generated tests for Argus Pitbull, a secure application environment technology. We documented our experience and lessons learned, and presented our results. Our work stimulated interest from researchers at the Defense Advanced Research Projects Agency (DARPA) and the Software Engineering Research Center (SERC). See [http://www.itl.nist.gov/div897/docs/automatic\\_software\\_test\\_generation.html](http://www.itl.nist.gov/div897/docs/automatic_software_test_generation.html).

Another area of interest is object oriented (OO) component testing. The goal is to improve software quality, reduce testing costs, and develop reliability estimates that software correctly adheres to its specification. Using our component integration test method, we automated the process of representing the OO specification in databases and generated executable tests. We also developed a Java rapid prototype machine to simulate implementation of the OO specification. See [http://www.itl.nist.gov/div897/docs/software\\_test\\_statistical.html](http://www.itl.nist.gov/div897/docs/software_test_statistical.html).



## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

# NETWORKS



(Standing) Richard Rouil, David Griffith, Nada Golmie, Kotikalapudi Sriram; (seated) Stephan Klink, Giuseppe Di Lorenzo, Oliver Borchert, SuKyoung Lee (not pictured), and SURF students Richard Su and Liliya Krivulina (not pictured) are studying management and control issues in future high-speed networks. The team has created the GMPLS/Lightwave Agile Switching Simulator (GLASS) that is being used by researchers both within and outside NIST to study new protocols to support intelligent, autonomous control of optical networks.

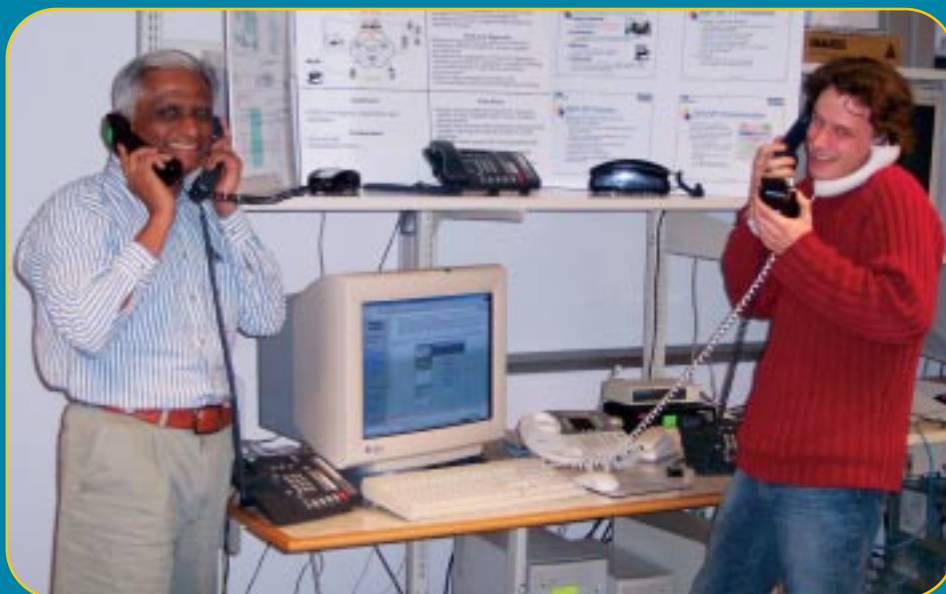
In FY 2003, ITL continued to conduct validation, simulation, and analysis of WPAN protocols. We characterized mutual interference between Bluetooth and IEEE 802.11b (WiFi) protocols. We developed and analyzed coexistence techniques, including scheduling and adaptive frequency hopping, to compensate for interference. We served as technical editor of the *Recommended Practices for Coexistence* for IEEE 802.15. We developed protocol implementation and conformance statements (PICS) and formal models in specification and description languages (SDLs) for IEEE 802.15.1 and 15.4. Modeling results shared with 802.15.4 uncovered numerous flaws in the draft specifications under consideration. Our work expedited the development of WPAN standards and improved the quality of specifications. The website is [http://www.antd.nist.gov/wlan\\_wpan.shtml](http://www.antd.nist.gov/wlan_wpan.shtml).

## NETWORKING FOR PERVASIVE COMPUTING

Networking is a significant component of ITL's pervasive computing program. We focus on two areas: the wireless communication protocols that enable devices in a ubiquitous computing environment to communicate, and the service discovery protocols (SDPs) that allow these devices to discover and invoke desired services. For the wireless protocols, we work with IEEE 802.15 Wireless Personal Area Network (WPAN) working group to develop short distance wireless protocol. For the service discovery protocols, we develop architectural models and characterize the behavioral and performance properties of some selected emerging protocols.

In the service discovery area, ITL developed models of Jini Networking Technology (Jini), Universal Plug-and-Play (UPnP), and the Service Location Protocol (SLP). We concentrated on analyzing the quality of service provided by these protocols under conditions of network failures. We studied the resilience of Jini and UPnP in the face of increasing communication failure, message loss, and node failure, and analyzed the performance of mechanisms to reduce latencies in detecting and recovering from failures. We investigated the recovery strategy used in Jini, which uses a leasing mechanism that grants a leaseholder access to services for a limited time (the lease period). A critical performance factor is choosing an appropriate lease period that involves tradeoffs among resource utilization, failure-





*Members of the NIST-SIP project work on technologies to expand the scope and application of Internet Telephony technology in areas such as context aware communications for mobile wireless devices and security techniques to enable programmable call control services. Pictured: Mudumbai Ranganathan and Jean Deruelle. Not Pictured: Olivier Deruelle, Jin Woo Jung, and Doug Montgomery.*

detection latency, and system size. We developed several self-adaptive leasing algorithms for Jini and demonstrated the effectiveness of automatic-leasing mechanisms for failure recovery. The website is <http://www.antd.nist.gov/sdp.shtml>.

## **AGILE SWITCHING INFRASTRUCTURES AND NETWORK MANAGEMENT**

In another focus area, ITL works on integrated control planes for optical network wavelength switching and the Internet protocol for Generalized Multi-Protocol Label Switching (IP/GMPLS). Our emphasis is on the evaluation and development of protection and restoration methods. We quantified the amount of resource required to support a fast optical path recovery in the event of network failures and contributed the results to the appropriate Internet Engineering Task Force (IETF) working group. We published papers on (1) the modeling methodology and the performance evaluation of shared protection schemes for GMPLS networks, and (2) network provisioning and routing under uncertainty. In addition, we are exploring the viability of the optical burst switching (OBS) technology for next generation core networks.

This year we released a new version of the GMPLS/Lightwave Agile Switching Simulator (GLASS) and a new implementation of GMPLS, NIST switch, on the Linux platform. We have also enhanced the NIST Network Emulation Tool, NISTnet, with new statistical methods and interfaces to large-scale Internet measurement data repositories. The website is [http://www.antd.nist.gov/agile\\_switch.shtml](http://www.antd.nist.gov/agile_switch.shtml).

## **INTERNET TELEPHONY / SIGNALING**

Another area of ITL interest is the design and evaluation of technologies to expand the capability and scope of emerging Internet telephony signaling standards. Projects include the design and development of architectures and standards for programmable Session Initiation Protocol (SIP) platforms and services; research and measurement of SIP signaling in wireless ad hoc networks; and test and evaluation of scalable presence mechanisms to enable location/context aware call control.

In FY 2003, we co-designed, with Sun Microsystems, a new JAIN/SIP 1.1 specification for Java SIP platforms. We designed and implemented the NIST-SIP 1.2 reference implementation and test tools. We integrated the NIST-SIP in the wireless ad hoc network (WANET) /NIST Distributed Testbed for First Responders. We conducted

simulation analysis of SIP in WANETs and published two research papers on proposed mechanisms to improve the hand-off performance for mobile users. ITL leads the development of industry standard software architecture and application programming interfaces (APIs) for Java-based SIP services. NIST-SIP has been adopted as a kick-off project in the Java.net community. Our NIST-SIP research platform is widely used throughout the research and development community. The website is [http://www.antd.nist.gov/it\\_voip.shtml](http://www.antd.nist.gov/it_voip.shtml).

## INTERNET INFRASTRUCTURE PROTECTION

Expediting the development and deployment of standardized Internet infrastructure protection technologies is another networking focus area. We are developing public specifications to secure the Internet naming infrastructure through our Domain Name System Security (DNSsec) project. Another effort is the development of large-scale virtual private network (VPN) modeling and analysis tools to characterize the performance and behavior of large-scale deployment of security services.

ITL leads the IETF community in the development of several technical specifications for DNSSec. This year we also developed and released the NIST IPsec/IKE Simulation Tool (NIIST) for detailed performance modeling of emerging IETF security protocols in large-scale networks. We also work with industry to expedite the development of standards for the protection of both content and resources in the Internet routing infrastructure. Our work is making a difference in two areas, Domain Name System (DNS) and Border Gateway Protocol (BGP), which are two critical vulnerabilities in today's Internet infrastructure. We lead the IETF effort to advance the DNSSec specification toward full Internet standard status, and we initiated new projects aimed at expediting the development and standardization of BGP security mechanisms. We also provided industry with tools to evaluate the performance impact of security services in large-scale deployments. The website is <http://www.antd.nist.gov/iipp.shtml>.

## WIRELESS AD HOC NETWORKS

The goals of this ITL project are to develop new architectures and protocols for wireless ad hoc networks (WANETs), develop a distributed network for first responders applying WANET technologies, develop technologies for emerging public safety communications, and assess technology for ultra wideband (UWB). A WANET is a collection of stationary/mobile nodes with wireless communication and possible multi-sensory capabilities. These networks have commercial applications, and some are mission-oriented networks, including first responder communications.

In FY 2003, we prototyped several major functionalities for public safety communications, including self-organization networks, multihop routing, audio/video streaming, short messaging, sensor data communications, voice over IP over the public switched telephone network (PSTN) to wireless handheld devices (PDAs), and geolocalization. We applied WANET technologies to the NIST Distributed Testbed for First Responders. We implemented Real-Time Transport Protocol (RTP) and frame synchronized packet protection to allow high-quality real-time video transport over WANETs. We further expanded WANET architecture to include a cellular-based architecture with mobile bases and nodes, and developed a metric for measuring mobility in WANETs. For the Defense Advanced Research Projects Agency, we wrote a comprehensive report on the merits and drawbacks of UWB and its potential applications. Our initiatives in developing requirements and standards for public safety communications are making a significant impact in government and industry. The website is [http://www.antd.nist.gov/wahn\\_home.shtml](http://www.antd.nist.gov/wahn_home.shtml).

## QUANTUM COMMUNICATIONS TESTBED

ITL worked with other NIST laboratories in the NIST Quantum Communications Testbed program to develop an infrastructure for distribution of quantum encryption keys. We developed a free space optical wavelength division multiplexing link and quantum channels, and necessary software for generation, distribution, and use of quantum encryption keys. (See the Quantum Information section of this report.)

## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

# INFORMATION ACCESS

## HUMAN LANGUAGE TECHNOLOGY

**B**y facilitating the creation of relevant measurement methods and standards, ITL is accelerating the development of technologies that allow intuitive, efficient access, manipulation, and exchange of complex information. Projects in human language technology include the Text REtrieval Conference (TREC) series, Advanced Question and Answering for Intelligence (AQUAINT), Translingual Information Detection, Extraction, Summarization (TIDES), automatic content extraction, machine translation, meeting transcription, the effective, affordable, reusable speech-to-text project, and speaker/language recognition.

Initiated in 1992, our TREC series is the premier workshop/evaluation series that supports the information retrieval community. In addition to common task-based individual experiments, TREC provides a forum for the exchange of research ideas and a means to accelerate technology transfer. With participation from 93 organizations from 21 countries, TREC 2002 featured six evaluation tracks, including an Arabic cross-language track that demonstrated that algorithms are of sufficient maturity to commercialize. We also prepared for six evaluation tracks for the TREC in November 2003. Our related AQUAINT program focuses on advancing the state of the art of question answering to the full range of complex questions asked by humans. In FY 2003, we tested the ability of question answering systems to engage in interactive dialogue; this laid the groundwork for a new kind of information retrieval testing.



*Darrin Dimmick, Trudy Cummings, and Lori Buckland provide the technical support for the ongoing Text Retrieval Conference (TREC) project.*

In support of the Defense Advanced Research Project Agency (DARPA), TIDES (Translingual Information Detection, Extraction, and Summarization) program, NIST coordinated a "surprise" language evaluation involving information retrieval, summarization, information extraction, and translation; for this, the choice of Hindi as the surprise language was revealed just prior to the evaluation, allowing researchers only a few weeks to adapt their systems to focus on this chosen language. For the TIDES topic detection and tracking project, we ran an evaluation for topic detection, realizing a dramatic improvement in new-event detection. For the DARPA Effective, Affordable, Reusable Speech-to-text (EARS) program, we performed speech-to-text and metadata evaluation for broadcast news and conversational



telephone speech, making a breakthrough in word error rates and in the development of metadata extraction from speech.

For the National Security Agency, through our Automatic Content Extraction (ACE) project, we are advancing the state of the art in automatically extracting content from newswire, broadcast news, and newspapers. In FY 2003, we conducted supporting evaluations for entity and relation extraction. This laid the groundwork for content extraction in Arabic and Chinese. In our machine translation project, we ran evaluations from Chinese to English, Arabic to English, and Hindi to English. For our meeting transcription project, we collected data for a speech-to-text evaluation, making progress in meeting recognition

technologies. Our speaker/language recognition work progressed; we ran evaluations and documented continued improvements in performance in FY 2003. The website is <http://www.itl.nist.gov/iad/programs.html#Human>.

## BIOMETRICS TECHNOLOGY

Mandated by the USA PATRIOT Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002, ITL's biometrics program focuses on fingerprint and face recognition testing, multimodal biometrics evaluation and system design, and biometrics standards. (See the Biometric section of this report.) The website is <http://www.itl.nist.gov/iad/programs.html#BIOMETRICS>.

## MULTIMEDIA TECHNOLOGY

To advance technologies for accessing and using multimedia information, ITL actively participates in standards development, video retrieval, and visualization and virtual reality for manufacturing. In FY 2003, we continued our leadership positions on standards committees such as the Moving Picture Experts Group (MPEG) and Web3D Consortium. We established and chaired an MPEG-7 profile definitions and rules group. We developed web-based utilities to generate/register MPEG-7 profile schemas. We created the NIST MPEG-7 Interoperability Testbed, with more than 200 members. Our MPEG work provides industry with a profile mechanism for transfer to the marketplace.

Video retrieval is another ITL focus area. We accomplished a major upgrade in the size and quality of data. We added the task of semantic feature identification, in addition to shot boundaries. The NIST video retrieval evaluations are becoming well known, with 32 participants in FY 2003. Our visualization and virtual reality for manufacturing project progressed. We serve as a member of the



*Perrine Roucoux, Charles Sheppard, and Christophe Kern are shown in the NIST Smart Space demonstrating control of several appliances using a prototype implementation of a flexible user interface standard developed for IT accessibility.*



Web3D Board of Directors. We incorporated a VRML/X3D translator into the prime X3D tool, which is now used by virtually all people working with X3D. We also co-chair the Medical Working Group within the Web3D Consortium, laying the groundwork for medical applications in Web3D. The website is <http://www.itl.nist.gov/iad/programs.html#Multi>.

## INTERACTIVE SYSTEMS TECHNOLOGY

ITL is providing metrics, standards, and test methodologies to improve the usability of interactive systems. Projects include WebMetrics, Industry USability Reporting (IUSR), voting standards, novel intelligence from massive data, human robot interactions, the Digital Library of Mathematical Functions (DLMF), and accessibility standards.

For our WebMetrics tool suite, we improved WebCAT, our category analysis tool. In our IUSR project, our Common Industry Format (CIF) was adopted as a national standard (ANSI / INCITS 354) in November 2001; this year we drafted a CIF-R (CIF for Requirements) document. Several companies now use the CIF for usability testing, and the IUSR currently has 312 members. For the ITL voting standards effort, we initiated a draft report on human factors, usability, and accessibility for voting. (See the Voting Program section of this report.) Our research in human robotic interactions advanced as we conducted data collection at Army facilities and experienced robotic search and rescue events. For the DLMF, we established a new interface to VRML files, leading to better 3D interactive visualization of mathematical functions. We continued our participation in the INCITS V2 Technical Committee, which is developing alternative interfaces for people with disabilities. We also developed a prototyping environment using Smart Space technology, progressing toward universal accessibility standards. The website is <http://www.itl.nist.gov/iad/programs.html#Users>.

## SMART SPACE TECHNOLOGY

ITL is advancing smart space technologies and accelerating their deployment by providing a modular testbed for integration, interoperability, architecture develop-



*Brian Antonishek videotapes a robot's activity in a rubble environment during a simulated urban search and rescue evaluation; this is part of the human-robot interaction data collection.*

ment, data collection, and performing experiments. Projects include our NIST Smart Space Testbed and single molecule manipulation and measurement.

In FY 2003, we made improvements to our Smart Data Flow middleware, with a simplified installation system and simplified construction of data flow charts. We integrated improvements into the prototype Meeting Room. Our new microphone array of 64 microphones is better integrated, easier and less expensive to replicate, easier to deploy, and more durable. We implemented device/user discovery protocols for accessibility; our prototype will be integrated with INCITS V2 architecture for accessibility and universal access. We deployed high-speed, real-time data acquisition/processing clusters to the NIST Chemical Sciences and Technology Laboratory and the NIST Physics Laboratory. We also produced many invited talks and papers. A significant impact of our work is the increasing visibility of the NIST Smart Space program. The website is <http://www.nist.gov/smartspace>.

## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

# INFORMATION INTEGRATION

**ITL** is providing new IT measurement methods and characterizations that further the advancement of digital information preservation and interchange. Projects in our assured content program include quantum communications and the electronic health record. Our assured use program includes biometrics and document control technologies. The information preservation program investigates both durability of storage and required fidelities of representation.

## ASSURED CONTENT

In FY 2003, we made significant progress in the development and integration of major quantum

communications components in support of the quantum research community. For our quantum key distribution (QKD) testbed, we completed the classical channel, developed and tested the quantum channel, and built and tested high-speed electronics that implement the QKD protocol management on a plug-in computer board. (For more information, see the Quantum Information section of this report.) The web page is <http://math.nist.gov/quantum/>.

Consistent with the NIST long-term programmatic interests in e-Health, we investigated critical impediments to widespread standardized electronic health record (EHR) deployment. We see an emerging need for measurement methods in health system

workflow/record flow. These methods will ensure the widespread, effective adoption of a uniform functional model for the EHR. Our initial demonstration—specifically designed with portability in mind—lays instrumentation groundwork for identifying inefficient workflow/record flow circumstances in clinical settings. Our customers for this work are the states, agencies such as the U.S. Department of Health and Human Services, health record vendors, and medical clinics and practices. (See the Healthcare section of this report.)



*Mike Indovina and Rob Snelick (seated) are developing new methods for multimodal biometric user identification.*

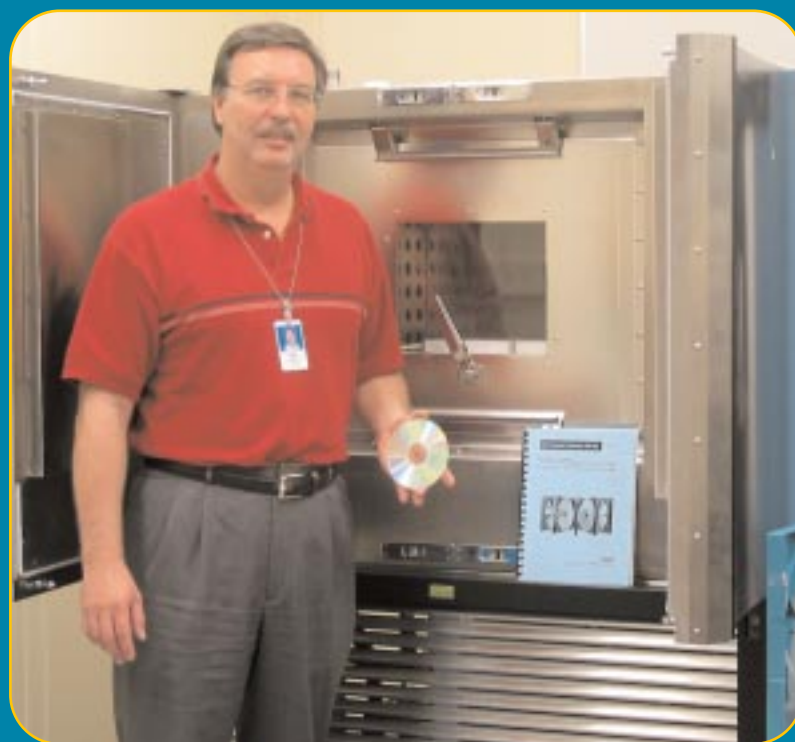
## ASSURED USE

We continued to develop standards and conduct research in biometric technologies. We led and expedited the Common Biometric Exchange File Format (CBEFF)/BioAPI standards efforts within the INCITS M1 and ISO/JTC1 SC37 programs of work. We submitted three data format standards for initial review. We advanced the harmonization of Unix/Linux BioAPI ports; the Unix/Linux base promotes standard open biometric architectures. (See the Biometrics section of this report.) Our efforts accelerated standards-based biometrics for border crossings and transportation workers. We also co-sponsored the Biometric Consortium Conference (BC2003) in September; this conference has become the largest biometrics conference in the world. The website is <http://www.itl.nist.gov/div895/isis/biometrics.html>.

We identified fresh approaches for insider threats to e-documents. An insider threat is defined as “a compromise of computer and electronic document systems by trusted agents of the targeted organization.” In February 2003, we co-sponsored and organized, with the National Security Agency (NSA) Advanced Research and Development Activity, a workshop entitled Advanced Countermeasures for Insider Threat. More than 120 government and vendor representatives attended the workshop, which presented 30 speakers and 10 vendor demonstrations. Participants shared insights on the nature of insider threats within government, government intelligence, and private sectors. The workshop was also designed to increase participation in an NSA grants competition. There is interest in exploring technology solutions to the insider problem for digital documents; the problem is first and foremost a systems integration issue that requires approaches broader than conventional computer security. Technology areas include digital rights management, biometrics, and portable electronic document system design.

## INFORMATION PRESERVATION

Through our work with both industry consortia and government agencies, we are making significant contributions to ensure the long-term preservation of digital information. Current and developing projects include a media longevity study, an interoperability study, and development of guidelines and standards for archival storage media, systems, and networks. We developed a test package for the DVD industry to test interoperability between discs and drives, and completed a study on the state of interoperability among DVD drives. This test plan is being used by DVD manufacturers to enable better interoperability among discs and drives in an industry-wide effort lead by the Optical Storage Technology Association (OSTA). We also published a significant document giving guidelines to archivists and librarians on the care and handling of optical media.



*Fred Byers authored a popular new publication on the care, handling, and preservation of CDs and DVDs for use by librarians and archivists.*





*Barry Hershman checks security plans for the Convergent Information Systems Division.*

We initiated a significant media longevity study in collaboration with the Library of Congress. The results of this testing will help government agencies choose the best media for their archival needs. We participated in the formation of the Government Preservation Working Group, which will use the longevity results and consult with industry to develop an Archival Grade DVD specification.

We published a paper entitled "High Precision Measurement of Reflectance for Films Under Substrates" in *Optical Engineering* magazine; the text describes a precise measurement for the traceable industrial standard for DVD reflectance. This work received NIST's Jacob Rabinow award.

In collaboration with the DVD Association, we hosted the 4th Annual DVD Conference in June. This event brought together more than 120 government and industry representatives from around the world to view and discuss the latest in DVD technology. The website is <http://www.itl.nist.gov/div895/isis/datas-torage.html>

The lack of quality metrology for motion imagery impedes development of imaging systems and inhibits information preservation for compressed imagery. We work with the Moving Picture Experts Group (MPEG), the Entertainment Technology Center, and government agencies (e.g., the National Imagery and Mapping Agency [NIMA]) to develop quality metrology. We led the verification tests for MPEG's next-generation video codec and ran the high definition parts of these subjective tests in our laboratory in the fall of 2003. With NIMA and others, we are developing a Motion Image

Quality (MIQ) metric. We designed and ran experiments to quantify MIQ and expect significant follow-on research. We served as an organizer of the SPIE Conference on Visual Information Communications and Processing in January 2003, which drew 80 speakers. We contributed papers at SPIE on digital cinema measurements, display metrology, and the Tactile Graphic Display (TGD), which was licensed to the State University of New York for research and commercialization. See <http://www.itl.nist.gov/div895/>.



## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

# MATHEMATICS

**ITL** provides technical leadership within NIST in state-of-the-art analytical and computational methods for solving scientific and engineering problems of critical interest to U.S. industry. To do this, we (a) collaborate closely on a wide variety of projects with scientists in the NIST Laboratories, and (b) develop techniques, tools, and facilities that improve the computational science environment both at NIST and at large.

## APPLIED MATHEMATICS

ITL applied mathematicians work in close collaboration with NIST scientists in the development, analysis, and solution of mathematical models of physical phenomena. These collaborations exhibit tremendous variety. We are modeling high-speed machining processes, developing methods for the registration of LADAR (laser RADAR) scans of construction sites, studying the stability of quantum wires, and developing new methods for multiple sequence alignment in bioinformatics. Areas of significant impact include the development of improved wireless communication systems. More than 215 copies of our software for the determination of optimal signal sets in the context of realistic noise models have been distributed.

We maintain a particular emphasis on applications in materials science. This year we extended the applicability of phase field models for alloy solidification, which we pioneered in the 1990s, to new problem domains. For example, in collaboration with the NIST Metallurgy



*Tim Burns (center) discusses high strain rate materials testing with NIST collaborators Dick Rhorer (right) and Debasis Basak. The Kolsky Bar facility is being used to develop data for the development and validation of accurate simulation models.*

Division, we developed models for the study of electrodeposition in multi-component systems as well as elastic effects on surface stress in two-phase systems. Another significant advance in our program in image reconstruction occurred in FY 2003 with the development of a new, highly effective technique for the recovery of texture in image deblurring. The method is based upon a new metric for image smoothness that can be efficiently computed. Our new Poisson Singular Integral method can robustly reconstruct texture in cases where other deblurring methods fail completely. The website is <http://math.nist.gov/mcsd/>.



*Adele Peskin (seated) demonstrates scientific visualization tools enabling remote collaboration to colleague Abbie O'Gallagher.*

## HIGH PERFORMANCE COMPUTING AND VISUALIZATION

High performance parallel computing is a key enabling technology for modern scientific discovery. We work closely with NIST scientists to develop highly efficient parallel computational models in a wide variety of areas including nanostructures, cement flow, and atomic properties. We also develop tools to enable such computations. A recent example is Screen Saver Science, a Java/Jini-based environment for developing distributed applications that can execute on otherwise idle network nodes (e.g., when their screen savers are active).

Visualization is a critical tool for gaining understanding of scientific data, whether the data is the result of physical measurement or output from large-scale computational

models. The centerpiece of our efforts in this area is a highly capable immersive visualization laboratory featuring two floor-to-ceiling screens and stereo head-tracked goggles. This year we used this facility to study the dynamics of smart gels in collaboration with the NIST Chemical Science and Technology Laboratory. The molecular-level 4D visualizations that we developed led to new understanding of how shake gels are formed. This understanding is expected to lead to new exotic foods, cosmetics, medicines, and sensors. The website is <http://math.nist.gov/mcsd/savg/>.

## MATHEMATICAL SOFTWARE

To improve the environment for computational research within NIST and the larger scientific community, ITL develops tests and makes available mathematical software tools and related information services. Such tools span the range from fundamental mathematical components to fully integrated problem-solving environments for particular applications. Active projects include the following:

- TNT: Template Numerical Toolkit for numerical linear algebra in C++
- MATRAN 95: Fortran 95 interface to linear algebra software



*Howard Hung and Clarissa Ferraris (BFRL) inspect cement samples; ITL is working with the Building and Fire Research Laboratory on a searchable cement properties database that also includes digital versions of actual cement aggregate.*

- PHAML: Parallel Hierarchical Adaptive Multi-Level solution of partial differential equations
- OOMMF: Object-Oriented Micromagnetic Modeling Framework
- OOF: Object-Oriented Finite Element modeling for materials with complex microstructure.

FY 2003 saw the initial releases of MATRAN and PHAML. OOMMF has now been referenced in more than 100 scientific papers, including one cited by the Institute of Physics as a top ten physics result of 2002. Our software continues to generate many downloads. For example, in the last year we logged the following: TNT 9,000; JAMA (a Java-based linear algebra library) 8,800; OOF 2,000; and OOMMF 1,600. Our web services, including the Guide to Available Mathematical Software (GAMS), saw 5.4 million page downloads from more than 440,000 hosts during the last year. The website is <http://math.nist.gov/>.

## DIGITAL LIBRARY OF MATHEMATICAL FUNCTIONS

ITL is leading the development of the Digital Library of Mathematical Functions (DLMF), a comprehensive, authoritative web-based interactive reference on the special functions of applied mathematics. The DLMF significantly updates and modernizes the NBS *Handbook of Mathematical Functions (with Formulas, Graphs, and Mathematical Tables)*, 1964, edited by M. Abramowitz and I. Stegun. This handbook remains a technical bestseller and is among the most widely cited of all mathematical publications. When operational in



*Andrew Reid and Steve Langer are developing the next generation virtual laboratory for the modeling of materials with complex microstructure.*

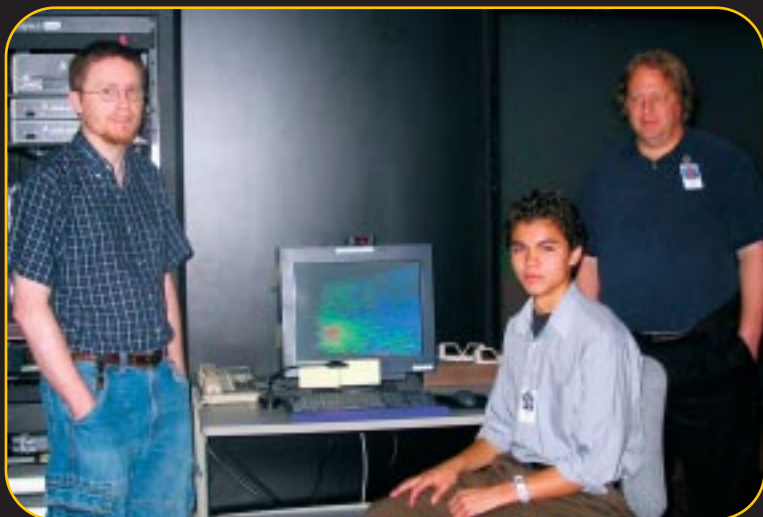
2005, the DLMF will provide standardized notations, definitions, and properties for special functions, with online traceability to NIST. It will also be available in print and CD/DVD versions.

The core of the DLMF is a database of mathematical properties compiled by some 40 external authors, editors, and validators. In FY 2003, 28 chapter drafts were accepted as ready for independent validation, while 11 chapters remain in various stages of revision and editing. We developed a math-aware search system and produced hundreds of graphics. We also initiated an XML-based translation system to enable the production of highly interactive web pages from the author's LaTeX input. The website is <http://dlmf.nist.gov/>.



## ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

# STATISTICS



*Terry Griffin, student Mathew Hoppe (seated), and Alan Heckert use the Reconfigurable Advanced Visualization Environment (RAVE) for data analysis.*

## BAYESIAN METROLOGY

**ITL** is advancing measurement science and technology by formulating and developing statistical theory and methodology for metrology. Bayesian Statistics provides a unified framework for optimally combining information from multiple sources, resulting in highly efficient experimental designs and statistical analyses. Projects include new Bayesian methods for metrology, expert elicitation for uncertainties, models, and designs, and Bayesian software and software testing.

In FY 2003, we provided eight implementations of Bayesian metrology on NIST research projects. We developed three elicitation tools (all interactive, graphical) and made four additions to our software suite. We presented seven talks, wrote four articles for refereed journals, and authored an invited chapter on Bayesian metrology for the *Encyclopedia of Statistics, Volume 6*. We published the first module of *A Bayesian Metrology*

*Casebook* with case studies and tutorials on the web. To translate this methodology into scientific application, we also conducted three courses at NIST in Bayesian methods for metrology, teaching more than 80 scientists. With our enlarged repertoire of methods, NIST is recognized as a premier locus for Bayesian metrology. The website is <http://www.itl.nist.gov/div898/bayesian/homepage.htm>.

## KEY COMPARISONS

A second focus area is the development and application of new statistical methods for the design and analysis of Key Comparisons (KCs). International KCs serve as the technical basis for acceptance of measurements by member laboratories participating in the Mutual Recognition Agreement (MRA) of the National Metrology Institutes (NMIs) worldwide. These, in turn, are the basis for international trade because specifications written in one country can be fulfilled in terms of the official units of measurement of another nation under this mutual recognition.

In FY 2003, we provided statistical expertise on KCs to ten NIST scientific projects and issued three final reports. We distributed two new software products via the web, as well as case studies that highlight statistical issues in KCs in nontechnical terms. We presented seven talks and authored eleven articles (seven for refereed journals) on KCs. We drafted a policy on statistics for KCs. We produced the first statistically developed methodology for artifacts with linear drift and the first rigorously derived methodology to link a KC with regional comparisons. We made the first definitive comparison of methods for determining KCRV (reference value) and uncertainty, and we conducted the first definitive review of methods for determining nonequivalent laboratories. All of this contributes to a solid statistical basis for supporting NIST scientists in the international venue. The website is <http://www.itl.nist.gov/div898/projects/keycomp.htm>.



## IT PERFORMANCE EVALUATION

ITL statisticians are applying statistical methods to evaluate information technology (IT) performance. Projects include statistical modeling for networks, statistical tools for biometrics, statistical basis for comparing software with experts, and statistical design for computer forensics.

This year we presented five talks/posters and wrote seven articles (four for refereed journals). We also developed a new software tool for extreme values. We focused network monitoring and performance metrics on distribution tails. We developed a statistically sound method for combining *black box* algorithms to optimize performance. We introduced experimental design principles to the IT community engaged in computer forensics. We made a significant impact through our contributions to document understanding, biometrics, and computer forensics projects in ITL. The website is <http://www.itl.nist.gov/div898/itperf/homepage.htm>.

## PROCESS CHARACTERIZATION

Working with NIST scientists and their industrial partners, ITL statisticians characterize complex instruments, systems, and processes in mathematical terms. Projects include the statistical characterization of high-speed optoelectronics devices, statistical models for subatomic particles, and statistics for the analysis of the World Trade Center (WTC) collapse.

In FY 2003, we developed the first algorithm for estimating time-base distortion and realization of random jitters to provide internal self-correction for high-speed optoelectronic devices. This demonstrated the feasibility of proposed calibration service for high-speed optoelectronics devices. We enabled and characterized new measurement technologies for subatomic particle lifetimes, essential to advancing the study of subatomic particles. We provided four statistically sound experimental designs for critical NIST experiments to provide

input into the WTC collapse modeling and analysis, optimizing the information in data inputs to the WTC analysis. We also presented five talks and authored or coauthored seventeen articles for refereed journals. The website is <http://www.itl.nist.gov/div898/character/homepage.htm>.

## COLLABORATION AND SRMS

As a core contribution to metrology and science at NIST, ITL statisticians provide collaborative research and support for NIST research and measurement services, including the NIST Standard Reference Materials (SRMs) and Calibration Programs. This involves individual collaborations with NIST scientists on research projects where optimal experiment design, statistical modeling, and data analysis contribute to improved measurement processes.

In FY 2003, we contributed to the certification of 54 SRMs; an additional 32 SRMs are in the certification process. During the year, we are engaged in collaborative research with 33 of the 38 scientific divisions at



*Jeffrey Fong and Jim Filliben, members of a NIST investigation team for determining the probable causes of the collapse of the World Trade Center (WTC) twin towers, pose behind part of a damaged three-column panel that used to be Panel #224 of the WTC North Tower in the middle of its east face between the 92nd and 95th floors. The panel, re-designated by NIST as S-10, currently sits at the NIST Gaithersburg site as part of a large number of damaged steels that were salvaged from Ground Zero and shipped to NIST following the September 11, 2001, disaster.*



Jim Filliben, Alan Heckert, Nell Sedransk, and Will Guthrie, Statistical Engineering Division, present the first copy of the NIST/SEMATECH e-Handbook of Engineering Statistics CD to NIST Director Arden Bement (seated).

NIST. We established a new policy for the development and certification of software for SRM analysis, issuing modern mass calibration guidelines for metrologists worldwide. We streamlined the certification process for frequently produced SRMs. We participated in the NIST-wide quality program for calibrations and reviewed an SRM Business Practices proposal. We rewrote mass calibration software and guidelines in English and Spanish that are now available on CD. The websites are <http://www.itl.nist.gov/div898/consult/consult.html> and <http://www.itl.nist.gov/div898/projects/srm.htm>.

## EDUCATION

ITL provides education and training that gives NIST researchers the statistical tools necessary to improve the quality of experimental design and analysis at NIST. Averaging 25-40 NIST scientists per course, we conduct a full schedule of standard and advanced courses and workshops in experimental design, functional and exploratory data analysis, Bayesian analysis, regression analysis, simulation, and specialized software. We conduct courses for

industry and a course for metrologists. Also offered are educational opportunities via web products and technical guidelines. Additionally, we ensure that our summer students (nine in FY 2003) receive an education in applied statistical research and in statistical applications to interdisciplinary science that will serve them well in their future research.

Issued in 2002, the *NIST/SEMATECH e-Handbook of Engineering Statistics* continues to be a top citation for web searches on "engineering statistics." ITL teamed up with International SEMATECH, a consortium of worldwide major semiconductor companies, to develop the web-based guide for engineers, scientists, businesses, researchers and teachers who use statistical techniques in their work. The *e-Handbook* updates NBS Handbook 91, *Experimental Statistics* (all-time #2 NIST best-seller), and also provides direct incorporation of "bundled" software for immediate user access and utilization, plus web publication of resources. This year we published the *e-Handbook* as a CD and distributed 1,000

copies. We also co-authored a Chapter on Statistical Methods for the *Digital Library of Mathematical Functions*. The website is <http://www.itl.nist.gov/div898/handbook/index.htm>.

## INFORMATICS AND HIGH-D STATISTICS

A new initiative focuses on high-dimensional modeling, software for high-dimensional data (data mining and visualization), with particular application to proteomics and bioinformatics. In FY 2003, we conducted background learning sessions and acquired software for high-D prediction. We participated in three conferences, presented two talks, and authored six articles for refereed journals. We prepared three new courses to be offered at NIST. With the NIST Materials Science and Engineering Laboratory, we established a statistical basis for design that was presented to a polymers industry consortium. More collaboration with NIST laboratories is planned as we expand our research in these exciting new areas.



## SELECTED CROSS-CUTTING THEMES

# BIOMETRICS

**ITL** is assisting government and industry in the development and deployment of biometric technologies through evaluation, standards, and research. Mandated by the USA PATRIOT Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002, our biometrics program centers around fingerprint and face recognition testing, multimodal biometrics evaluation and system design, and biometrics standards.

## FINGERPRINT AND FACE RECOGNITION TESTING

ITL has been researching and developing biometric technologies for more than 30 years. Our researchers led the critical evaluations of fingerprint and face recognition technologies that resulted in a report to Congress recommending a dual approach to screen visa applicants and visa holders entering the United States. Co-authored by NIST and the Departments of Justice and State, the report recommends the use of at least four, and preferably ten, fingerprints to positively identify visa applicants and a dual system of face and fingerprints to verify the identities of visa holders at points of entry into the United States. The Department of Homeland Security (DHS) is using the results of this report to design US-VISIT, the new entry/exit system to better protect U.S. borders.

In FY 2003, we continued to provide fingerprint interoperability standards and evaluation technology for the Department of Justice, the FBI, DHS, the National Institute of Justice, developers, vendors, and law enforcement organizations. We performed fingerprint verification and identification tests with very large, operational databases. We installed a Cogent system for performing these tests and prepared for 2, 4, 6, and 8-finger testing. We consulted with DHS to help optimize an upgrade path for US-VISIT from 2 plain to more fingerprints. Lastly, we developed plans, schedules, and



*(Front to back) Ross Micheals, Charles Wilson, Mike McCabe, and Steve Otto examine one of the fingerprint matching systems, which is part of the biometrics evaluation program.*

tests for Fingerprint Vendor Technology Evaluation (FpVTE) 2003, an independently administered technology evaluation of fingerprint matching, identification, and verification systems that we are conducting for the U.S. Department of Justice. The website is <http://www.itl.nist.gov/iad/894.03/fing/fing.html>.

Face recognition testing is another area of ITL expertise. In light of major applications for homeland security, we conducted the 2002 Face Recognition Vendor Test (FRVT), the largest public state-of-the-art performance assessment of face recognition systems to date. We published FRVT 2002 results as NISTIR 6965 (<http://www.frvt.org/>). Next year we will help integrate face and multi-vendor verification into US-VISIT.

## MULTIMODAL BIOMETRICS EVALUATION AND SYSTEM DESIGN

Using a multimodal testing approach, we developed a multimodal testing methodology and system design, and presented a conference paper on our work. Next year we will develop a prototype for a multimodal biometric system.

## ACCELERATION OF BIOMETRIC STANDARDS DEVELOPMENT

Consumers need biometric-based high performance, interoperable systems (e.g., standards-based) developed in a timely fashion. In the absence of timely standards developments, migration from proprietary systems to these open-systems, standards-based solutions will be more difficult and expensive. Therefore, standards are the cornerstone of our biometrics program. NIST is responding to post-Sept. 11, 2001, market requirements for open systems standards by accelerating development of formal, national, and international biometric standards. Our strategy to accelerate the development of biometric standards includes:

- Leverage existing consortia standards (e.g., BioAPI and CBEFF)
- Chair the national biometric standards body (INCITS Technical Committee M1 on Biometrics)
- Chair the international biometrics standards body (ISO/IEC JTC 1/SC 37 on Biometrics)
- Provide expert technical leaders for critical standards projects
- Support required administrative infrastructure (e.g., ISO/IEC JTC 1/SC 37 Secretariat)

- Work through biometric standards "incubators" (e.g., Biometric Consortium)
- Promote fast processing of consortia specifications into national/international standards.
- Initiate development of technical implementations and software development for Conformity Assessment.

INCITS M1 is developing a portfolio of biometric data interchange, interoperability, and performance testing standards and also intends to elevate existing key consortia standards to formal national and international standards. The current INCITS M1 program of work includes biometric data interchange formats, exchange framework formats, application programming interfaces, application profiles, and performance testing and reporting standards. INCITS M1 is also the U.S. TAG to ISO/IEC JTC 1/SC 37 on Biometrics, which is developing a similar portfolio of standards at the international level.

The INCITS M1 web site is  
[http://www.incits.org/tc\\_home/m1.htm](http://www.incits.org/tc_home/m1.htm).

The ISO/IEC JTC 1/SC 37 website is <http://www.jtc1.org> (select SC37).

The ITL Biometrics Resource Center website is  
<http://www.nist.gov/biometrics>.



## SELECTED CROSS-CUTTING THEMES

# CRITICAL INFRASTRUCTURE PROTECTION

**P**rotecting the nation's vital infrastructure is a top priority of the federal government. Recent power outages, natural disasters, the increased incidence of Internet viruses and worms, as well as the tragedy of September 11, 2001, have all contributed to a sense of urgency about the nation's physical infrastructures and the information systems that keep them going. Infrastructures such as communications systems, electricity and other energy services, financial services, water delivery systems, and transportation networks have become increasingly automated and interlinked. This creates new vulnerabilities such as equipment and network failures, human error, weather and other natural causes, and physical and cyber attacks.

Consistent with our mission and long-standing IT security responsibilities, ITL focuses on security standards, guidance, metrics, and testing to help protect our nation's critical infrastructures. We support federal departments and agencies under the Federal Information Security Management Act of 2002 and other legislation that assigns to NIST responsibility to develop security standards and guidelines for sensitive, unclassified federal systems. Through the development of standards and testing programs, we are helping IT users and vendors to build products that will better protect information and improve security. (See the Security section of this report.) These improved products, in turn, provide enhanced security of the communications and information processing backbone of our nation's critical infrastructures.



*ITL focuses on IT security standards and testing to help ensure the security of our nation's critical infrastructures.*

## SELECTED CROSS-CUTTING THEMES

# HEALTHCARE

**ITL** is working with the healthcare industry, government agencies, and academia to improve the quality of healthcare, reduce costs, and provide essential services through more effective use of information technology (IT). Although it is a major industry in the United States, the healthcare community has lagged behind other industries in the application of IT to improve the delivery of services. As part of the NIST Healthcare Strategic Focus Area, we are developing standards and measurements to ensure the security and privacy of electronic medical records, to provide conformance tests and methodologies for healthcare, and to develop new modes of communication for mobile healthcare providers. Four of our technical divisions contribute to this ITL cross-cutting initiative.

To launch our healthcare initiative, we conducted two conferences to receive initial industry input on healthcare needs and requirements. We sponsored an *Information Technologies for Healthcare: Barriers to Implementation*

*Workshop* in August 2002. Our *Pervasive Computing 2002 Conference* in October 2002 emphasized medical pervasive computing applications. Next we gathered information from a number of healthcare organizations, including the American Telemedicine Association, the American Academy of Family Physicians, the ANSI Health Informatics Standards Board, the Agency for Healthcare Research and Quality, Health Level Seven (HL7), and others. The needs of the healthcare industry identified in this process include conformance testing and certification, usability, privacy and security of electronic health records (EHR), and improved communications for mobile healthcare providers.

Projects in our e-Health initiative include HL7 conformance, conformance advisory, healthcare standards roadmap, security guidance, electronic patient records, and nomadic communications. In FY 2003, we developed HL7 V2/V3 conformance definitions, with the result that HL7 specifications were changed to support conformance. The HL7 Experimental Registry was finalized and is now available for use. ITL actively participates in standards development activities through the ANSI Health Informatics Standards Board, eGOV Consolidated Health Informatics, HL7, Connecting for Health, and others. We co-sponsored a workshop with the American Telemedicine Association to advance ocular telehealth standards. We developed a healthcare standards roadmap, metadata, schema, and initial prototype. We laid the groundwork for a common set of healthcare IT security practices. We drafted a report on the complexity, prospects, and constraints of EHR and identified barriers to EHR in small practices. We published novel research on signaling protocol for mobile ad hoc networks. Lastly, we developed a prototype of a context aware network; the nomadic prototype was downloaded by 1,300 organizations.

By contributing our expertise in standards development, conformance testing, usability, wireless communication, and security and privacy of information systems, ITL is making major contributions to the healthcare industry. The website is <http://www.nist.gov/ehealth>.



*ITL is working with the healthcare industry to apply information technology for improved delivery of healthcare services and reduced costs.*

## SELECTED CROSS-CUTTING THEMES

# QUANTUM INFORMATION

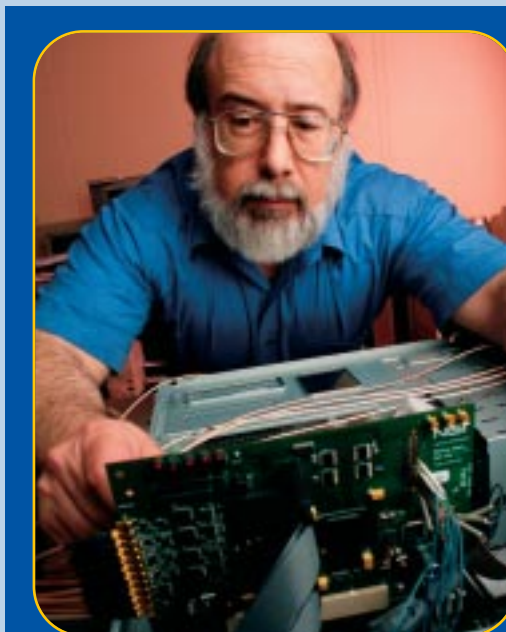
**ITL** is participating in the NIST Quantum Information program, which aims to develop a measurement and standards infrastructure to enable future information systems based on the principles of quantum physics. Working in collaboration with the NIST Physics and Electronics and Electrical Engineering Laboratories, ITL's goals are to understand the potential for quantum information to revolutionize information science, develop and test secure, commercial-grade quantum communications systems and protocols, and develop architectures and algorithms to enable the engineering and testing of quantum computer systems. ITL research in this area is supported in part by the Defense Advanced Research Program Agency and the NIST Competence Program. Five of ITL's divisions participate in three program areas.

## QUANTUM KEY DISTRIBUTION TESTBED

ITL is developing a testbed for the distribution of cryptographic keys using a quantum channel. The testbed is based on a free-space optical link between two buildings on the NIST campus. Bits of cryptographic key are transmitted using a beam of single polarized photons (the quantum channel). A second (classical) channel is also needed to implement the BB92 quantum key distribution (QKD) protocol. The properties of quantum physics make it possible to detect eavesdropping on the quantum channel, a critical property missing in classical systems. The NIST testbed will operate at 1.25 Gbps and is expected to yield about 1 Mbps of usable key when it is completed later this year, making it the fastest operational system to date. Such systems may enable practical one-time pad cryptography, the strongest cryptosystem known. In FY 2003, we completed the classical channel, developed and tested the quantum channel, and built and tested high-speed electronics for qubit data management.

## QUANTUM COMMUNICATION PROTOCOLS

A second research area involves the development and analysis of improved protocols for QKD, as well as for other tasks such as authentication. In FY 2003, we completed the software infrastructure for the NIST QKD testbed, studying methods for reconciling sifted keys in high-speed QKD, and completing an Application Programmer's



*Alan Mink verifies Quantum protocol signals on the high-speed electronics for the NIST Quantum Communication Testbed.*

Interface (API) for integrating QKD into applications. Our analysis of QKD protocols uncovered flaws in two recently published proposals, exposing the difficulty of developing truly secure QKD protocols. This year we also developed a new QKD protocol based on entanglement swapping.

## QUANTUM ARCHITECTURES AND ALGORITHMS

We are developing architectural concepts for the design of quantum computers and the implementation of quantum algorithms. In FY 2003, we developed quantum computer architectures appropriate for qubits realized via neutral atoms confined in optical lattices. This architecture supports nonlocal operations on multiple qubits using the notion of an entanglement bus. We developed a new optimization strategy for quantum circuits, demonstrating conditions in which costly measurement operations can be deferred. In addition, we developed a simulation tool for quantum circuits designed to study the propagation of errors in systems with imperfect gates. Finally, we delved deeply into quantum phenomena used to implement qubits themselves. Using a new parallel software tool based upon adaptive grid refinement, we computed a very challenging 30-node wave function of the Schrödinger equation for a Cesium atom under consideration for realizing qubits. The web page is <http://math.nist.gov/quantum/>.



## SELECTED CROSS-CUTTING THEMES

# VOTING PROGRAM



Working with the nation's diverse voting community, the mission of ITL's voting program is to enhance the capacity and performance of the nation's voting systems through the development and promotion of standards, measures, and technology. The goal of the program is to improve the election process and the voter experience. Mandated by the Help America Vote Act of 2002, the program consists primarily of intramural R&D and conformity assessment efforts. Additionally, ITL will support the Technical Guidelines Development Committee (TGDC), a group of 15 members that is chaired by the NIST Director. ITL leads a diverse group across NIST including personnel from five divisions in ITL, the Manufacturing Engineering Laboratory, Technology Services, and the Office of the Director. Our voting community customers include concerned citizens, the disabled, states and counties, voting equipment vendors, and independent testing authorities.

Projects within the voting program focus on human factors, security, hardware/software integration, computer forensics, laboratory accreditation, and TGDC support. In FY 2003, ITL networked with members of the election community, building rapport and learning issues and concerns. We initiated a human factors report, drafted a hardware/software integration standards white paper, investigated computer security needs, and examined the potential use of computer forensics for testing voting systems. We developed a roadmap/transition plan, met with state and local election officials, and hired a voting program manager. These actions laid the groundwork for an enhanced standards process for voting systems. Potential standards issues for voting systems include accessibility, usability, hardware/software issues, security, and statistical metrics. Next year, under the direction of the TGDC, we will initiate programs in response to issues identified during the past year.



# INDUSTRY AND INTERNATIONAL INTERACTIONS

**ITL's** research, measurement, and standards programs are greatly enhanced by our interactions with partners in industry, academia, government, and standards developers, both at home and abroad. Our program of work is enriched by our participation in many consortia and industry interest groups, including the following:

## AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI has served as administrator and coordinator of the U.S. private sector voluntary standardization system for 80 years. Thomas Rhodes and Lisa Carnahan serve on the ANSI Healthcare Informatics Standards Board (HISB), while Fernando Podio serves on the Homeland Security Standards Panel Steering Committee. NIST/ITL is an ANSI-accredited standards developer. Michael McCabe is the contact for ANSI/NIST-ITL 1/2000, *Data Format for the Interchange of Fingerprint, Facial, & SMT Information*.

## ASTM

ASTM (American Society for Testing and Materials) is a nonprofit organization that provides a forum for producers, users, ultimate consumers, and those having a general interest (representatives of government and academia) to meet on common ground and write standards for materials, products, systems, and services. Through the participation of Nien-Fan Zhang in Technical Committee E-11, ITL promotes quality in statistics.



*Ed Roback, Chief, Computer Security Division, spoke on "NIST Cyber Security Activities and Resources" at the Global InfoSec 2003 Summit at the United Nations in New York City on September 11, 2003.*

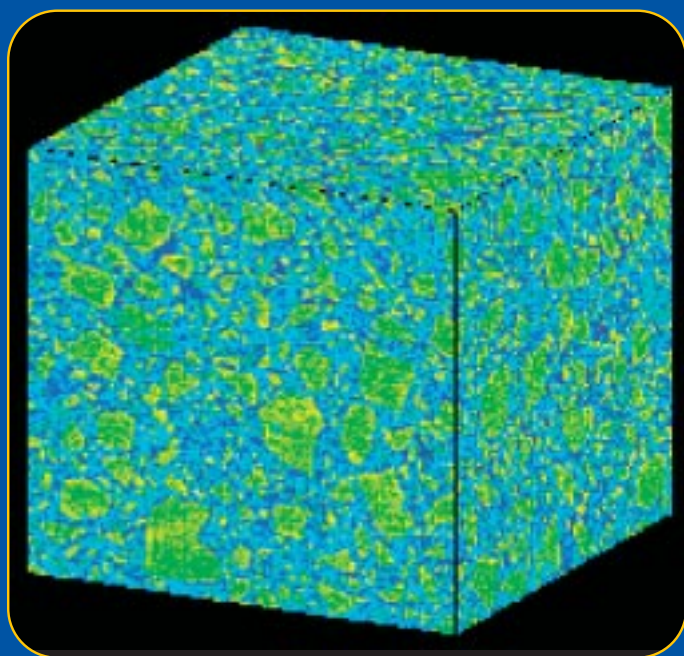
## BIOMETRIC APPLICATION PROGRAMMING INTERFACE (BIOAPI) CONSORTIUM

The BioAPI Consortium is an international organization of over 100 members including IT organizations, biometric vendors, and users. The consortium developed the BioAPI specification v1.1, ANSI/INCITS 358. Fernando Podio serves on the Steering Committee and chairs the BioAPI External Liaisons Working Group. As an open systems specification,

the BioAPI is intended for use across a broad spectrum of computing environments to ensure cross-platform support.

### BIOMETRIC CONSORTIUM (BC)

The NIST/National Security Agency BC serves as the federal government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology. Fernando Podio co-chairs the Biometric Consortium as well as the Biometric Interoperability, Performance, and Assurance Working Group.



*ITL is collaborating with the NIST Building and Fire Research Laboratory and several external partners to create a database of three-dimensional representations of hydrating cement, plaster of Paris, and common brick material obtained using x-ray microtomography. Shown here is a visualization of one of the datasets from this Visual Cement Dataset project.*

### CROSS INDUSTRY WORKING TEAM (XIWT)

The XIWT is a multi-industry coalition of IT companies that attempts to identify common issues and concerns in IT strategic directions and policy matters. ITL's participation assists in this process by providing technical guidance that bridges the gap between the research, standardization, and policy communities. Doug Montgomery represents NIST on the executive committee.

### DVD ASSOCIATION (DVDA)

The DVDA represents standards developers, software developers, disc and electronics manufacturers, government agencies, and content developers for DVD and associated technologies. Oliver Slattery and Fred Byers represent ITL. Through our representation, we facilitate standards, interoperability, and compatibility for writable DVD media, disc drives, and consumer electronic players.

### EGOV CONSOLIDATED HEALTH INFORMATICS

The Consolidated Health Informatics Initiative is the healthcare component of President Bush's eGov initiative. The committee facilitates the adoption of a common coding system for patient medical information, so that federal agencies will be able to exchange information without having to translate it into a new system. Tom Rhodes represents ITL on the committee. Through our participation, ITL is helping to standardize federal clinical health information.

### FORUM ON PRIVACY AND SECURITY IN HEALTHCARE (FPSH)

Sponsored by the National Information Assurance Partnership (NIAP, a joint National Institute of Standards and Technology and National Security Agency initiative) and the Healthcare Open Systems and Trial (HOST), the FPSH is incorporated as a nonprofit charitable organization consisting of participating members from approximately 50 healthcare organizations. Arnold Johnson represents ITL, which with support from the NIST

Advanced Technology Program (ATP) and NIAP, is developing guidance material and reference Common Criteria (CC)-based profiles to assist, demonstrate, and educate the healthcare community in specifying Protection Profile security requirements using the ISO/IEC 15408 CC standard.

### HEALTH LEVEL 7 (HL7)

HL7 is an ANSI-accredited standards developing organization that provides standards for the exchange, management, and integration of data to support clinical patient care and the management, delivery, and evaluation of healthcare services. Specifically, HL7 seeks to create flexible, cost-effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems. Lisa Carnahan, John Barkley, and Leonard Gallagher represent ITL in the HL7 Conformance Special Interest Group (SIG). Carnahan and Gallagher participate in the HL7 Modeling and Methodology Technical Committee, while Barkley and William Majurski contribute to the HL7 Templates SIG. Our expertise advances the interoperability of systems delivering healthcare services.

### HIGH DENSITY STORAGE ASSOCIATION (HDSA)

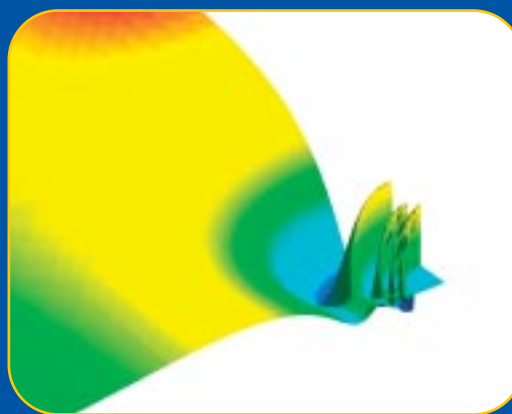
The HDSA has a well-defined charter to focus on automated, storage-centric technologies, known as jukebox or library storage, and acts as a centralized communicator among the industry, resellers, and users. The group identifies interoperability, connectivity, and compatibility issues and develops specifications to enhance the storage infrastructure. Oliver Slattery represents ITL, which provides a neutral platform to perform testing and development so the industry can improve the interoperability and performance of products for high-density data storage.

### INDUSTRY USABILITY REPORTING PROJECT (IUSR)

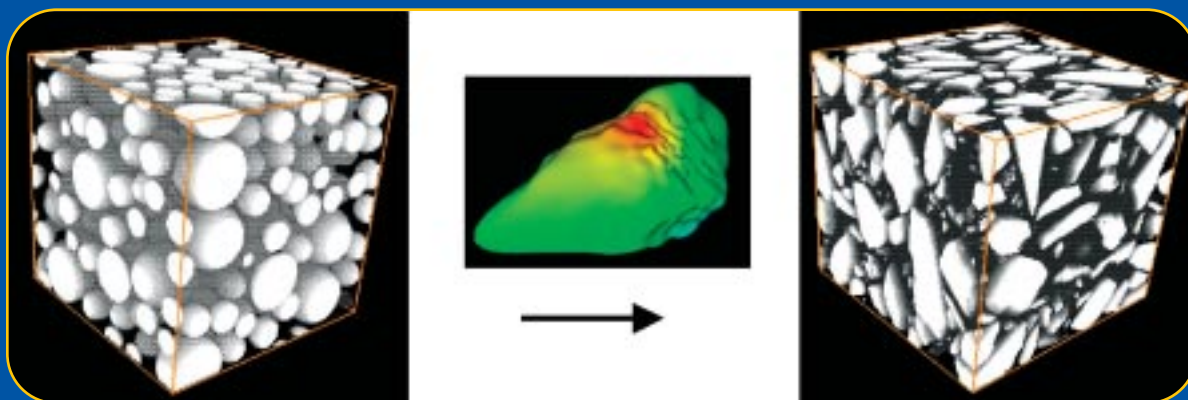
This NIST/industry collaboration resulted in the development of a Common Industry Format (CIF) for sharing usability data with consumer organizations. The reporting format was adopted as a national standard (ANSI / INCITS 354) in November 2001. Emile Morse, Jean Scholtz, and Sharon Laskowski lead the ITL effort and facilitate the international standardization of CIF.

### INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

The world's largest technical professional society, IEEE focuses on advancing the theory and practice of electrical, electronics and computer engineering, and computer science. Sharon Laskowski participates in P2001, Web Best Practices Working Group (WG). David Cypher, Robert Van Dyck, Nada Golmie, and Nader Moayeri participate in IEEE 802.15, WG for Wireless Personal Area Networks, and Moayeri also attends IEEE 802.16, WG on Broadband Wireless Access Standards. Mary Brady and Richard Rivello participate on IEEE 1073, Medical Device Communications. Larry Reeker participates in IEEE P1600.1, Standard Upper Ontology



*NIST Physics Laboratory researchers are using ITL's PHAML software for fast adaptive solution to the Schrodinger equation to examine the effect of trapping potential shape for quantum bits based on neutral atoms.*



*ITL is collaborating with scientists in the Building and Fire Research Laboratory to model the flow of particles in concrete. Here, a simplified model with idealized circular aggregate is improved using scanned models of actual aggregate (rocks). The result is both more realistic and computationally challenging.*

WG, and represents ITL on the Industrial Advisory Board of the Software Engineering Body of Knowledge (SWEBOK) project, which seeks to identify the body of knowledge of software engineering and to provide suitable access to that knowledge.

#### **INTERNATIONAL COMMITTEE FOR INFORMATION TECHNOLOGY STANDARDS (INCITS)**

INCITS's mission is to produce market-driven, voluntary consensus standards in a wide range of IT areas. Michael Hogan serves on the INCITS Executive Board and Standards Policy Board. Teresa Schwarzhoff and Jim Dray participate in TC B10, Identification Cards and Related Devices. Mike Rubinfeld chairs and Mike McCabe serves on TC L3, Coding of Audio, Picture, Multimedia and Hypermedia Information. Wo Chang, Charles Fenimore, and Rubinfeld participate in TG L3.1, MPEG Development Activity. Rubinfeld and McCabe are also on TG L3.2, Still Image Coding. Judy Newton serves on TC L8, Data Representation. Fernando Podio chairs and McCabe, Hogan, and Patrick Grother participate in TC M1, Biometrics. McCabe and Hogan are also on TG M1.1, Biometric Data Interchange Formats; Podio and Hogan serve on TC M1.2, Biometric Technical

Interfaces; Podio chairs and Hogan participates in TG M1.3, Biometric Application Profiles; Grother and Hogan are on TG M1.4, Biometric Performance Testing and Reporting; David Cooper participates in TC T3, Open Distributed Processing; Alicia Clay serves on TC T4, IT Security Techniques; and Sharon Laskowski and Charles Sheppard represent ITL on TC V2, IT Access Interfaces. Through these interactions, we contribute our expertise to the development of IT industry standards.

#### **INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP)**

ITL's Ronald Boisvert chairs the IFIP Working Group 2.5, Numerical Software, which strives to improve the quality of numerical computation by promoting international cooperation in the development of languages, guidelines, tools, and standards for numerical software.

#### **INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)**

The ISO is a worldwide federation of national standards bodies from some 140 countries, one from each country. Nien-Fan Zhang serves on the Committee on



Reference Materials (REMCO) WG1 for ISO Guide 35. Zhang and Nell Sedransk participate in the management group for ISO TC 69, Statistical Methods. Our contributions facilitate the development of international agreements that are published as International Standards.

### INTERNET ENGINEERING TASK FORCE (IETF)

ITL contributes to the technical development of the Internet through participation in the IETF, which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Doug Montgomery, Scott Rose, and Sheila Frankel participate in the Internet Area; David Griffith participates in the SUB-IP Area; Mark Carson, Leonard Miller, Nader Moayeri, and Montgomery participate in the Routing Area; Montgomery, Okhee Kim, Frankel, Nelson Hastings, and Tim Polk participate in the Security Area; Polk also chairs the PKI Using X.509 Working Group; and Montgomery and Mudumbai Ranganathan participate in the Transport Area.

### INTEROPERABLE MESSAGE PASSING INTERFACE (IMPI)

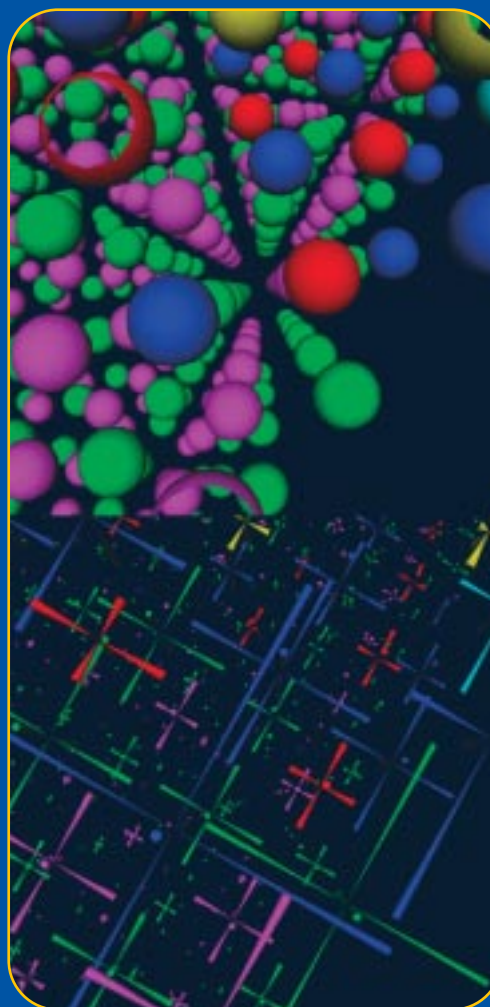
ITL actively participates in the development of standards and conformance testing for IMPI. William George, John Hagedorn, and Judy Devaney represent ITL; our contributions benefit industries that use a parallel code across different vendor systems, including the embedded computing community.

### JAVA GRANDE FORUM (JGF)

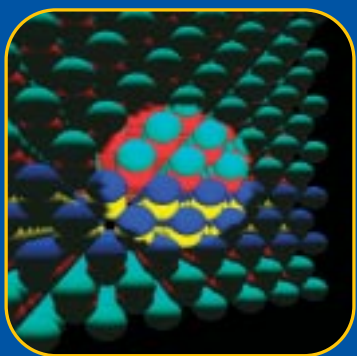
The JGF is an open working group of industrial, government and academic researchers, and software developers interested in improving the Java language and environment for technical computing applications. Roldan Pozo and Ronald Boisvert co-chair the Numerics Working Group, which works with Sun Microsystems to implement changes in Java's specifications which admit much faster execution (up to ten times faster) for computing-intensive applications.

### MICROMAGNETIC MODELING ACTIVITY GROUP (MUMAG)

muMAG is an organization of industrial, government, and academic researchers investigating fundamental issues in micromagnetic modeling through the establishment of standard problems for testing micromagnetic simulation software and the development of a public domain reference implementation of micromagnetic simulation software. Michael Donahue and Donald Porter represent ITL on the steering committee.



*Immersive scientific visualization is playing a key role in the study of materials at the nanoscale. Here, atoms in a particular nanostructure are displayed as balls (top) along with a representation of orbitals for the same structure (below).*



*ITL staff is developing a variety of tools for exploring scientific data in three-dimensional immersive visualization environments. Here, a virtual flashlight controlled by the orientation of a hand-held wand is used as a pointing device.*

#### **MOVING PICTURES EXPERTS GROUP (MPEG) INDUSTRY FORUM**

MPEG is a working group of ISO/IEC in charge of the development of standards for coded representation of digital audio and video. The MPEG Industry Forum is a nonprofit organization that strives to further the adoption of MPEG standards, by establishing them as well accepted and widely used standards among creators of content, developers, manufacturers, providers of services, and users. Wo Chang represents ITL.

#### **NATIONAL FILE FORMAT ADVISORY PANEL**

The National File Format Advisory Panel, which reports to the U.S. Secretary of Education, has been working on the National Instructional Materials Accessibility Standard (NIMAS). This standard will specify the file format to be used by publishers of textbooks and other instructional materials, in order to maximize accessibility to the material. Examples of accessibility issues include formatting the textbook files so they can be easily translated into Braille, correlating text and speech forms of material, and providing alternate presentations formats, such as those for students with learning disabilities. John Roberts represents ITL on the panel.

#### **NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)**

NIAP is a NIST/NSA partnership for testing methods and measures to ensure the quality of information security systems. Patricia Toth represents ITL. Our involvement helps to ensure that the security testing needs of federal and industry IT consumers and producers are met.

#### **NORTH AMERICAN OPEN MATH INITIATIVE (NAOMI)**

Open Math is a standard for communicating mathematical objects between computer programs. Bruce Miller represents ITL in this organization and in the Open Math Society.

#### **OBJECT MANAGEMENT GROUP (OMG)**

OMG is a nonprofit international consortium of 500 organizations whose mission is to research, develop, and promote the use of object-oriented technology for distributed systems development. John Barkley is ITL's principal representative to OMG.

#### **OPTICAL INTERNETWORKING FORUM (OIF)**

The OIF fosters the development and deployment of interoperable products and services for data switching and routing using optical networking technologies. David Su and David Griffith represent ITL in the Architecture, Internetworking, and Management groups.

#### **OPTICAL STORAGE TECHNOLOGY ASSOCIATION (OSTA)**

OSTA is an international trade association dedicated to promoting the use of writable optical technology for storing computer data and images. Xiao Tang represents ITL.

## ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS)

OASIS is an international consortium dedicated to accelerating the adoption of product-independent formats based on public standards. These standards include XML, HTML, and CGM as well as others that are related to structured information processing. Lynne Rosenthal, Lisa Carnahan, Michael Kass, and Mark Skall represent ITL. Our participation includes the development of conformance tests for these standards.

## SOCIETY FOR AUTOMOTIVE ENGINEERS (SAE)

SAE is a resource for technical information and expertise used in designing, building, maintaining, and operating self-propelled vehicles for use on land or sea, in air or space. Over 83,000 engineers, business executives, educators, and students from more than 97 countries share information and exchange ideas for advancing the engineering of mobility systems. Sandy Ressler participates in SAE-G13, Human Standards.

## SOCIETY OF MOTION PICTURE AND TELEVISION ENGINEERS (SMPTE)

SMPTE is an international technical society devoted to advancing the theory and application of motion-imaging technology. Wo Chang serves on W25, Metadata Description. Randall Easter participates in the Study Group on Conditional Access for Digital Cinema.

## WEB3D CONSORTIUM

The Web3D Consortium provides a forum for the creation of open standards for Web3D specifications and accelerates the worldwide demand for products based on these standards through the sponsorship of market and user education programs. Sandy Ressler represents ITL on the MPEG Development Activity and the Humanoid Animation Working Group.

## WORLD WIDE WEB CONSORTIUM (W3C)

The W3C is an international industry consortium created to lead the web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. Mark Skall serves on the W3C Advisory Committee. Tim Boland represents ITL on the Authoring Tools Working Group (WG), the Authoring Tools Accessibility WG, and the Cascading Stylesheets WG. Richard Rivello participates in the Document Object Model WG. Bruce Miller serves on the Math WG. Lynne Rosenthal, Mark Skall, and Sandra Martinez are involved in the Quality Assurance Activity. Martinez and Carmelo Montanez-Rivera participate in the Query WG. John Tebbutt represents ITL on the Schema WG, Wo Chang on the SYMM WG, and Martinez on the XML WG. Montanez-Rivera serves on the Extensible Stylesheet Language (XSL) WG. ITL's contributions facilitate web interoperability.

## X9

X9 develops, establishes, publishes, maintains, and promotes standards for the financial services industry in order to facilitate delivery of financial products and services. Morris Dworkin participates in X9F, Data and Financial Information Security, and X9F.1, Cryptographic Tool Standards and Guidelines. Elaine Barker, Lawrence Bassham, Sharon Keller, and Annabelle Lee serve as Editors in X9F.1. Elaine Barker attends X9F.3, Cryptographic Protocols, and Annabelle Lee participates in X9F.5, Digital Signature and Certificate Policy. Through participation in this forum, ITL promotes the security of the financial services industry.



*Visualization of a model rheometer (a device for measuring particle flow properties) under study using a quaternion-based dissipative particle dynamics code developed in collaboration with the NIST Building and Fire Research Laboratory.*



# STAFF RECOGNITION

## DEPARTMENT OF COMMERCE 2003 MEDAL AND NIST AWARDS



Left to right (seated): **Patrick Grother, Craig Watson, Elham Tabassi, Stephen Wood**; left to right (standing): **Ross Michaels, Martin Herman, Charles Wilson, Michael Garris**, all from the Information Access Division, and **Fernando Podio**, Convergent Information Systems Division, received the Department of Commerce Gold Medal for scientific/engineering achievement in the development of standards, testing methodology, and metrics for biometric technologies to be used for security the nation's borders.



Left to right: **Ron Tencati, Jeff Horlick** (NIST Technology Services), **Janet Jing, Ray Snouffer, Annabelle Lee, Randy Easter, Sharon Keller**, and **Gary Stoneburner**, all of the Computer Security Division, and inset **Larry Bassham**, Computer Security Division, and **Lisa Carnahan**, Software Diagnostics and Conformance Testing Division, received a Department of Commerce Silver Medal for leadership in conceiving, establishing, and operating the Cryptographic Module Validation Program and developing Security Requirements for Cryptographic Modules.



**William Guthrie, Nien Fan Zhang, N. Alan Heckert**, and **James Filliben**, Statistical Engineering Division, received a Department of Commerce Silver Medal for scientific achievement in the development and electronic publication of the NIST/SEMATECH *e-Handbook of Statistical Methods*, an interactive web resource for science and industry. Holding the CD version of the handbook are NIST Director **Arden Bement** and **Nell Sedransk**, Chief, Statistical Engineering Division.





**Tom Karygiannis**, Computer Security Division, received the Department of Commerce Bronze Medal for leadership in advancing and improving wireless and mobile security in the public and private sectors.



**John Roberts** (right) and **Oliver Slattery**, Convergent Information Systems Division, received the Department of Commerce Bronze Medal for scientific/engineering achievement in the develop-

ment of a new, low cost, refreshable tactile graphic display technology for the blind and visually impaired.

**Murugiah Souppaya**, Computer Security Division, received the Department of Commerce Bronze Medal for conceiving, developing, and fielding the Windows 2000 Professional Security Benchmark.



**Xiao Tang**, Convergent Information Systems Division, received the 2003 Jacob Rabinow Award for conceiving and developing an accurate calibration technique now used as a standard procedure for the manufacture of DVDs and optical discs worldwide.



## EXTERNAL RECOGNITION



**Elaine Barker**, Computer Security Division, was selected as an individual finalist for the Frank B. Rowlette Award for Individual Excellence, awarded annually by NSA. This prestigious award recognizes those who have made extraordinary contributions in the field of information security. A prolific writer and editor, Barker has authored, edited, co-authored, or co-edited eighteen ANSI and Federal Information Processing Standards (FIPS) cryptographic standards.

**Ronald Boisvert**, Chief, Mathematical and Computational Sciences Division, received the 2002 Keene State College (KSC) Alumni Achievement Award, which is given each year to one whose professional achievement in their chosen field brings honor to themselves and the college. Boisvert is the 31st winner of the award since its establishment in 1971.



**Ramaswamy Chandramouli**, Computer Security Division, received the best paper award for his authorship of "Specification and Validation of Enterprise Access Control Data for Conformance to Model and Policy Constraints." The Organizing Committee of the 7th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2003) presented the award.



**Alicia Clay**, Deputy Chief, Computer Security Division, was appointed a Vice-Chairman of the technical committee T4 - IT Security Techniques of INCITS, the InterNational Committee for Information Technology Standards, which is an ANSI-accredited standards organization. T4 is the USA Technical Advisory Group to ISO/IEC JTC 1 SC 27, IT Security Techniques. Clay received a second award when Sigma Xi selected her for membership in the 2004-2006 Sigma Xi College of Distinguished Lecturers.





**Charles Fenimore**, Convergent Information Systems Division, was selected for membership in the 2004-2005 Sigma Xi College of Distinguished Lecturers. Since 1937, Sigma Xi has presented its Distinguished Lecturers as an opportunity for chapters to host visits from outstanding individuals who are at the leading edge of science.

Sigma Xi members support the talks, with additional support from the American Meteorological Society, the National Academy of Engineering, and the Society for Risk Analysis.

**James Filliben**, Statistical Engineering Division, was named a Fellow of the American Statistical Association. Filliben was recognized "for exemplary work in statistical consulting with physical scientists and engineers, for leadership in the development of statistical software, and for technical contributions of national importance."



**Timothy Grance**, Group Leader, Systems and Network Security Group, Computer Security Division, received a 2003 Federal 100 Award for providing principal technical direction to the development of information security technical

guidelines and serving as key reviewer to ensure overall quality and consistency with legal, policy, and other existing security guidelines.

**Michael Hogan**, Office of the ITL Director, received the ANSI Edward Lohse Information Technology Medal, which recognizes the contributions of an individual to the national and international IT standards community through leadership and fostering of cooperation among the bodies involved in global standardization. Hogan is ITL's and NIST's



management and policy representative on the InterNational Committee for Information Technology Standards (INCITS) and its predecessor organization, ANSI Accredited Standards Committee X3.



**Stuart Katzke**, Computer Security Division, received the 2003 Mathematics and Computer Sciences award from the Washington Academy of Sciences Board of Managers. The award designates Katzke as a Fellow of the Academy and was presented under the Academy's Annual Awards Program for Scientific Achievement.

**Fernando Podio**, Convergent Information Technology Division, was selected for a three-year term of office as Chairman of the new subcommittee ISO/IEC JTC 1/SC 37, Biometrics (SC 37). The scope of the subcommittee is the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems.

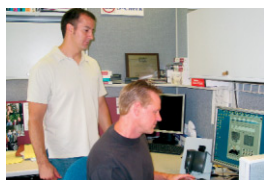


**Edward Roback**, Chief, Computer Security Division, received a 2003 Federal 100 Award from *Federal Computer Week*. The award cited Roback's role in raising awareness about ITL's security tools and expertise, and in coordinating the division's portfolio of products.

Accepting on behalf of a government team, Roback also received a 2003 SecurE-Biz award from the CIO Advisory Board and Awards Committee. The awards recognize government programs that have helped further e-business Transformation, one of the key goals of the President's Management Agenda.

# THE PEOPLE OF ITL

AOLAT ADEDEJI TONAN AGBOTA NEGA ALEMAYEHU DANIEL ALLEN BRADLEY ALPERT PAUL AMMANN DANIEL ANDERSON BRIAN ANTONISHEK JULIEN AUBE ANA AVILES RICHARD AYERS ERIC BAER SIMON BAIK STEPHANY BAILEY KOICHIRO BAN BRUCE BARGMEYER ELAINE BARKER WILLIAM BARKER JOHN BARKLEY LAWRENCE BASSHAM ISABEL BEICHL GEORGE BENNETT JAVIER BERNAL BARRY BERNSTEIN MELISSA BETANCOURT ROBIN BICKEL PAUL BLACK DEBORA BLACKSTONE CHAD BLOMQUIST JAMES BLUE DUANE BOES ROBERT BOHN RONALD BOISVERT FREDERICK BOLAND MARVIN BORCHARDT OLIVER BORCHERT PAULINE BOWEN MARY BRADY ALAN BRANNICK RICHARD BRAUN TANYA BREWER-JONEAS RONNIE BRITTON ELEAZER BROMBERG TAMARA CAHEN CHRISTOPHER BROWN LORI BUCKLAND LORNA BUHSE STEPHEN BULLOCK TIMOTHY BURNS WILLIAM BURR FREDERICK BYERS DOMENIC CAPPABIANCA ALFRED CARASSO LISA CARNAHAN ROBERT CARPENTER TANYA CARR MARK CARSON SARA CASWELL RAMASWAMY CHANDRAMOULI JOSHUA CHANG SHU-JEN CHANG WO CHANG MICHAEL CHERNICK NICOLAS CHEVROLIER YOU CHO JAE CHUNG ANTHONY CINCOTTA MARY CLARK ALICIA CLAY KEVIN COAKLEY KENDRA COLE LESLIE COLLICA TRACY COMSTOCK KIERAN CONDON JOYCE CONLON ANDREW CONWAY RYAN COOKE DAVID COOPER CHRIS COPELAND JOHN CORNELL JOHN COSTELLO DAVID COTRELL CEDRIC COULON MARY CROARKIN TRUDY CUMMINGS RICHARD CURTAIN DAVID CYPHER CHRISTOPHER DABROWSKI ERIC DALCI PAMELA DAVIS ANDRE DEPRIT JEAN DERUELLE JUDITH DEVANEY DIPAK DEY ANDREW DIENSTFREY GIUSEPPE DI LORENZO ALDEN DIMA DARRIN DIMMICK GEORGE DODDINGTON DONNA DODSON KIRK DOHNE MICHAEL DONAHUE JAMES DRAY MORRIS DWORKIN RANDALL EASTER CYNTRICA EATON ADABEZE ESIOLU ALLAN EUSTIS BRUCE FABIJONAS CHARLES FENIMORE DAVID FERRAILO JAMES FILLIBEN ANTOINE FILLINGER JONATHAN FISCUS LARRY FITZWATER PATRICIA FLANAGAN MARY FLOYD ELIZABETH FONG JEFFREY FONG JOHN FOUNTAIN JULIEN FRANIATTE SHEILA FRANKEL JUDITH FRYE OLIVIER GALIBERT LEONARD GALLAGHER KATHLEEN GALLO STEPHANIE GANTT AKASH GARG JOHN GAROFOLLO MICHAEL GARRIS JOHN GARY SAUL GASS SERBAN GAVRILA LEONARD GEBASE CAMILLO GENTILE WILLIAM GEORGE HAMID GHARAVI SUBHRA GHOSH DAVID GILSINN SEAN GINEVAN DONALD GISH AFZAL GODIL SYLVIA GOLDEN ALAN GOLDFINE ALAN GOLDMAN NADA GOLMIE LOURDES GONZALEZ LAURA GOODING TIMOTHY GRANCE MARTHA GRAY CHRISTOPHER GRIFFIN JONATHAN GRIFFIN TERENCE GRIFFIN DAVID GRIFFITH PATRICK GROTHOR AIHUA GUO KATHARINE GURSKI WILLIAM GUTHRIE BARBARA GUTTMAN SEUNG-ILL HAAN JEROME HAERRI JOHN HAGEDORN ROBERT HAGWOOD TIMOTHY HALL JAN HANNIG DONNA HARMAN GERLINDE HARR VICKIE HARRIS ERIC HARVEY JOAN HASH NELSON HASTINGS KRISTI HAWES NATHANIEL HECKERT MIKKO HEIKKERO SYDNEY HENNRARD MARTIN HERMAN BARRY HERSHMAN PEGGY HIMES ALMA HINTON ROBERT HITCHO MICHAEL HOGAN DIANE HONEYCUTT MATHEW HOPPE PAMELA HOUGHTALING YING-PO HSIAO VINCENT HU JENNIFER HUCKETT WILLIAM HUFF ELIZABETH HUGHES RICHARD HUGHES HOWARD HUNG FERN HUNT MICHAEL INDOVINA MICHAELA IORGA HARIHARAN IYER STANLEY JANET WAYNE JANSEN JANET JING ARNOLD JOHNSON RAGHU KACKER KAREN KAFADAR ATHANAS KARYGIANNIS DOMINIK KASPAR MICHAEL KASS STUART KATZKE ANTHONY KEARSLEY CHRISTOPHER KEITHLEY SHARON KELLER JOHN KELSEY JOHN KELSO EDWARD KENNEDY HOWARD KERMISCH CHRISTOPHE KERN PETER KETCHAM LAWRENCE KEYS CHUL KIM ELAINE KIM OKHEE KIM RICHARD KISSEL LUKE KLEIN-BERNDT ARTHUR KLEPCHUKOV KENTON KLINE STEPHAN KLINK EMANUEL KNILL JOSEPH KONCZAL HSIAO-MING KOO VLADIMIR KOROLEV DAVID KUHN SRIKANTA KUMAR JOHN KUNTZ BYUNG-JAE KWAK MARY LAAMANEN ANDREW LANE STEPHEN LANGER CHRISTOPHE LAPRUN MARIANNE LARKIN JONATHAN LASKO SHARON LASKOWSKI JAMES LAWRENCE TONY LE CANDICE LEATHERMAN NANCY LEATHERMAN DENNIS LEBER YANN LEBLEVEC ANNABELLE LEE CALEB LEE JULIEN LEFORT ANDREW LEIFER STEFAN LEIGH ELIZABETH LENNON



WALTER LIGGETT HUNG-KUNG LIU BENJAMIN LIVELSBERGER SUSAN LOAR SAMUEL LOMONACO BENJAMIN LONG TERRANCE LOSONSKY DANIEL LOZIER JOHN LU RICHANG LU CHRISTOPHE LUCAS JAMES LYLE GORDON LYON KATHY LYONS-BURKE KATHERINE MACFARLAND WILLIAM MAJURSKI DONALD MALEC JOCELYN MALONES VLADIMIR MARBUKH KAREN MARSHALL ALVIN MARTIN ROBERT MARTIN-ROLSKY SANDRA MARTINEZ LAUREN MATTHEWS LEONARD MAXIMON ROBERT MCCABE ANDREW MCCAFFREY MARJORIE MCCLAIN JANET MCCULLOCH-BASS GEOFFREY MCFADDEN STEVEN MEAD KATHRYN MEADOW-ORLANDS LUIS MELARA ROSS MICHEALS MARTIAL MICHEL BRUCE MILLER LEONARD MILLER KEVIN MILLS ALAN MINK WILLIAM MITCHELL NADER MOAYERI FRANCESCO MOGGIA CARMELO MONTANEZ-RIVERA DOUGLAS MONTGOMERY STANLEY MOREHOUSE KIMBERLY MORGAN ROY MORGAN EMILE MORSE CAROLYN MULFORD BRUCE MURRAY ANASTASE NAKASSIS BERTRAND NDZANA JUSTIN NEAL JAMES NECHVATAL PATRICIA NELSON JUDITH NEWTON HAN KIM NGO CATHY NGUYEN ANNA NHAN CHRISTIAN NIEVES ALEXEI NIKOLAEV SUDALIN NOTTHAM AGNES O'GALLAGHER DIANNE O'LEARY PATRICK O'REILLY JEFFERSON OFFUTT VADIM OKUN FRANK OLVER STEVEN OTTO PAUL OVER DAVID PALLETT TWINKLE PAMNANI DANNY PAN SANGWOO PARK YOLANDA PARKER HARRIET PECK ADELE PESKIN HERBERT PATTERSON JAN-WEN PENG JOANNE PERRIENS CHRYSTINE PHAM JONATHON PHILLIPS MICHELE PITTS FERNANDO PODIO MARGARET POLINKOVSKY WILLIAM POLK BERT PORTER DONALD PORTER FRANCES PORTER VITAL POURPRIX ROLDAN POZO NICOLAS PRATZ MARK PRZYBOCKI REBECCA QUINN STEPHEN QUIROLGICO SHIRLEY RADACK NICOLAS RADDE MUDUMBAI RANGANATHAN OLIVIER REBALA LARRY REEKER MICHAEL REILLY ERIC RENAUT SANFORD RESSLER THOMAS RHODES ANN RICKERDS KELSEY RIDER CLEMENT RIDORET RICHARD RIVELLO EDWARD ROBACH JOHN ROBERTS KATHLEEN ROBERTS CEDRICK ROCHET MARK ROSE SCOTT ROSE JOAN ROSENBLATT LYNNE ROSENTHAL RONALD ROSS PERRINE ROUCOUX RICHARD ROUIL JULIE ROUZAUD EUGENE ROWE MYRON RUBINFELD ANDREW RUKHIN CRAIG RUSSELL BERT RUST VITO SABIA XENIA SAEZ PATRICIA SALPINO DENISE SANDERS GREGORY SANDERS DARRIN SANTAY STEVEN SATTERFIELD GEORGE SAUER BONITA SAUNDERS ROBERT SCHMIECH JEAN SCHOLTZ TERESA SCHWARZHOFF MEGAN SEAMAN NELL SEDRANSK PHILIPPE SENELAS CLEMENT SEVEILLAC CHARLES SHEPPARD KATHERINE SHERWIN DA SHI KELLY SHUGGARS JAMES SIMS MARK SKALL OLIVER SLATTERY PATRICK SMELLER ROBERT SNEELICK STANLEY SNOUFFER DOROTHY SNYDER IAN SOBOROFF WON-KYU SOHN YEUNGJOON SOHN DAVID SONG JABIN SONG NAH-OAK SONG HAROLD SORRELL JUAN SOTO MURUGIAH SOUPPAYA TERESA SPLAIN JOLENE SPLETT SIVA SRINIVASAN KOTIKALAPUDI SRIRAM VINCENT STANFORD EDWIN STEEBLE GILBERT STEWART GARY STONEBURNER WILLIAM STRAWDERMAN DAVID SU VERA SUIT FRANCIS SULLIVAN SUZANNE SULLIVAN MARIANNE SWANSON RAMAZAN TABAN ELHAM TABASSI CERYEN TAN HAI TANG XIAO TANG JOHN TEBBUTT RONALD TENCATI ANDREW TESCHER AMIR SOLTANIAN TIRANCHI BLAZA TOMAN KATHY TON-NU AUDREY TONG PATRICIA TOTH SAMUEL TRAHAN SHARON TRAVIS UMUT ULUDAG ROBERT VAN DYCK DOMINIC VECCHIA JULIEN VIET ELLEN VOORHEES JOHN WACK CHIH-MING WANG QIMING WANG KELLY WATKINS CRAIG WATSON CHARLES WAYNE SHARON WENTLING DOUGLAS WHITE ELIZABETH WILLIAMS JEANNETTE WILLIAMS CHARLES WILSON MARK WILSON CLARE WITTE STEPHEN WOOD JOAN WYRWA GRACE YANG JAMES YEN JEFFREY YOUNG MICHELLE YOUNG ABDOU YOUSSEF JARVIS YU JIAN YUAN JULIE ZANON SUSAN ZEVIN NIEN-FAN ZHANG JIAN ZHENG

**NOTE:** Reference to specific commercial products or brands is for information purposes only; no endorsement or recommendation by the National Institute of Standards and Technology, explicit or implicit, is intended or implied.



