



Technical Accomplishments

2002



*Enabling a
Better Future*

NISTIR 6909

NIST

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

C O N T E N T S	
Director's Foreword	1
ITL at a Glance	4
ITL Research Blueprint	6
Accomplishments of our Research Program	7
Foundation Research Areas	8
Selected Cross Cutting Themes	29
Accomplishments of our Services Program	33
Industry and International Interactions	35
Staff Recognition	42

NISTIR 6909
NOVEMBER 2002



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

DIRECTOR'S FOREWORD

Let me introduce you to the Information Technology Laboratory (ITL). As one of the National Institute of Standards and Technology (NIST) Laboratories, our mission is to develop and promote measurement science, standards, and technology for information technology (IT) in order to enhance productivity, facilitate trade, and improve the quality of life. We develop computer security standards and guidelines for the federal government in fulfillment of a legislative mandate. And, new homeland security legislation, the USA Patriot Act of 2001 (P.L.107-56) and the Aviation and Transportation Security Act (P.L.107-71), mandate our research and standards development work in biometrics. Working in partnership with industry, academia, government, and consortia, we develop and demonstrate tests, test methods, reference data, proof-of-concept implementations, and other IT infrastructure technologies. Our goal is to enable the future of the U.S. IT industry to produce products and services that are high quality, reliable, interoperable, and secure.

ITL also supports and contributes to major NIST Strategic Focus Areas (SFAs). In support of the Healthcare SFA, we have begun work on the development of a healthcare standards roadmap, which will provide a set of web services and infrastructure for establishing, populating, searching, maintaining, and administering healthcare standards information. With other NIST laboratories, we participated in the establishment of the Distributed Testbed for First Responders as part of the Homeland Security SFA. Also significant is our Quantum Communication Testbed Facility in support of the NIST Nanotechnology SFA.



*Susan F. Zevin,
Acting ITL Director*

In critical research and standards areas, ITL made significant contributions in Fiscal Year (FY) 2002. Industry, government, academia, and consortia recognized the valuable contributions of our work, including:

Statistical Methods e-Handbook – ITL and International SEMATECH collaborated to publish the online resource e-Handbook of Statistical Methods, which provides a comprehensive overview of statistical methods, including experiment design, data analysis, and quality control, for engineers and scientists worldwide;

Active Networks Project – A research team from ITL received the “Bytes for the Buck” award from the Defense Advanced Research Projects Agency (DARPA) Active Networks program for the project judged most productive and cost effective. The ITL team developed a standard means to specify processor demands for mobile computer programs;

Common Industry Format Specification – The National Committee for Information Technology Standards (NCITS) adopted ITL’s Common Industry Format for Usability Test Reports (NCITS 354). This document standardizes the types of information captured in the software development testing process;

Computer Forensics – ITL released the National Software Reference Library (NSRL) Reference Data Set, which, together with our Computer Forensics Tool Testing project, provides valuable resources for the law enforcement community investigating crimes involving computers;

Digital Library of Mathematical Functions (DLMF) – Collaborating with other NIST laboratories and the National Science Foundation, ITL is developing an interactive web-based information resource on the special functions of applied mathematics;

Distributed Testbed for First Responders - ITL is working with NIST’s Building and Fire Research Laboratory and the Manufacturing Engineering Laboratory to build a NIST Distributed Testbed for First Responders that will integrate a number of technologies, including advanced communication technologies, novel spatial localization techniques to allow localization and tracking of important assets, and smart sensor networking to detect and predict the evolution of fires and chemical, biological, radiological, nuclear or high-yield explosive (CBRNE) attacks and the dangers they pose to the health of victims and first responders at the disaster site;

Guidance on Wireless Network Security and Security Certification and Accreditation (C&A) of Federal Information Technology Systems - ITL is developing guidelines for federal and industry users on these significant topics and others;

Homeland Security - ITL contributed to a joint report, submitted to Congress by the Attorney General, Secretary of State, and NIST by mandate of the USA

Patriot Act and the Enhanced Border Security and Visa Entry Reform Act. The report assesses the actions and considerations needed for issuing machine-readable tamper-proof U.S. visas and other travel documents and for deploying equipment to the U.S. borders to allow biometric comparison and authentication of the documents. ITL provided an appendix that outlined appropriate standards for biometric accuracy, tamper resistance, and interoperability;

Multi-Laboratory Single Molecule Measurement and Manipulation Program - The NIST Smart Flow Distributed Processing Middleware platform generates speech recognition reference data and supports pervasive computing standards work at ITL. It also provides high-speed data acquisition and pattern recognition for research at NIST’s Physics and Chemical Science and Technology Laboratories;

NIST Refreshable Tactile Graphic Display - ITL has developed, in cooperation with the National Federation of the Blind, a new, refreshable tactile graphic technology that allows blind and visually impaired users to view images using the sense of touch. Future applications include viewing graphics, science, engineering, mathematics, education, and design graphics, both technical and artistic;

Quantum Communication Testbed - In collaboration with the NIST Physics and Electronics and Electrical Engineering Laboratories, ITL is developing a quantum communication testbed facility for technology assessment and integration, showcasing hardware and protocols for cryptographic key distribution based on commercially feasible technologies;

Role Based Access Control (RBAC) – An independent economic impact study, sponsored by NIST, estimated that ITL’s RBAC research saved U.S. industry \$295 million and accelerated industry’s adoption of this advanced access control method by a year. Three ITL researchers received the 2002 Department of Commerce Gold Medal for this work;

Wireless Personal Area Networks (WPANs) – ITL contributed significantly to a new standard for WPANs approved by the Institute of Electrical and Electronics Engineers (IEEE). The approval of IEEE 802.15.1 (the Bluetooth Core Specification) advances the wireless technology that operates in the 2.4 GHz frequency band and provides voice communications at 64 bit/s and data transfers up to 732 kbit/s at distances up to 10 meters; and

XML/Document Object Model (DOM) – ITL and the World Wide Web (W3C) Consortium released the first version of the DOM Conformance Test Suite, Level 1 Core. We developed the test suite using XML technology and automated test generation methods, adding DOM to five other test suites for XML technology standards.

In addition to our core research and standards programs, this report highlights our laboratory-wide initiatives. ITL co-sponsored two major Biometrics Consortium Conferences this year and led the biometrics standards development process. Our critical infrastructure protection (CIP) initiative includes security standards and testing. Pervasive computing efforts focus on smart space integration, pervasive software tools, and pervasive networking technology. We also started a laboratory-wide initiative in healthcare.

ITL also provides research collaborations and technical services to the NIST laboratories. Our mathematicians and statisticians support work in the other NIST laboratories and perform crucial services such as modeling and certification of Standard Reference Materials (SRMs). Further, we provide vital services to the entire NIST community, including networking, high performance computing, support for desktop computers and workstation machines, the telephone system, and a host of other infrastructure activities.

In addition to our research contributions, ITL made significant progress in enhancing the provision of IT services to the NIST staff. We launched our information technology assistance center (iTAC) to provide a central-

ized help desk for IT questions and solutions. And, in cooperation with the NIST Director of Administration/Chief Financial Officer organizations, we enabled the implementation of the new NIST Grants Management Information System. We also implemented business continuity and disaster recovery plans for core IT business functions. And, finally, based on the maturity of its functions and accomplishments, ITL created a new NIST Chief Information Officer (CIO) and Services organization, which will stand alone by the end of 2002.

Finally, ITL respects its diverse workforce and works to enhance the quality of life for all members of the staff. Our quarterly Town Meetings keep the staff informed of our progress and activities. The ITL Diversity Committee sponsors division open houses, a holiday party, and a summer picnic for the staff. We also present ITL awards to individuals who made significant contributions to the research, service, and administrative programs of the laboratory. We work to ensure the safety of our workplace, holding cleanup days and safety seminars. Our Summer Undergraduate Research Fellowships (SURF) program brought 15 deserving undergraduates to ITL last summer to pursue research opportunities. See our website at <http://www.itl.nist.gov>.

Thank you for your interest in the Information Technology Laboratory. In partnership with industry, government, and academia, we will continue to enable 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*

ITL AT A GLANCE



*Kamie Roberts
Acting ITL
Deputy Director*

OUR MANAGEMENT TEAM

Susan F. Zevin, *Acting ITL Director, ITL Deputy Director, and Acting NIST Chief Information Officer (CIO)*

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

Bruce Rosen, *Office of the CIO*

Robert Glenn, *IT Security Office*

Yvonne DiCarlo, *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*

Victor McCrary, *Chief of Convergent Information Systems Division*

Raymond Hoffmann, *Chief of Information Services and Computing 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.

OUR MISSION

To develop and promote measurement, standards, and technology for information technology (IT) to enhance productivity, facilitate trade, and improve the quality of life. We also provide NIST with high-quality information technology services and 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 498 (includes part-time and faculty appointments), supplemented by 111 guest researchers (as of September 21, 2002)
- total authorization for fiscal year 2002 budget of \$95.3M, all sources (as of September 30, 2002)
- 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
- hardware, software, and network support to NIST staff
- mathematical and statistical consulting services

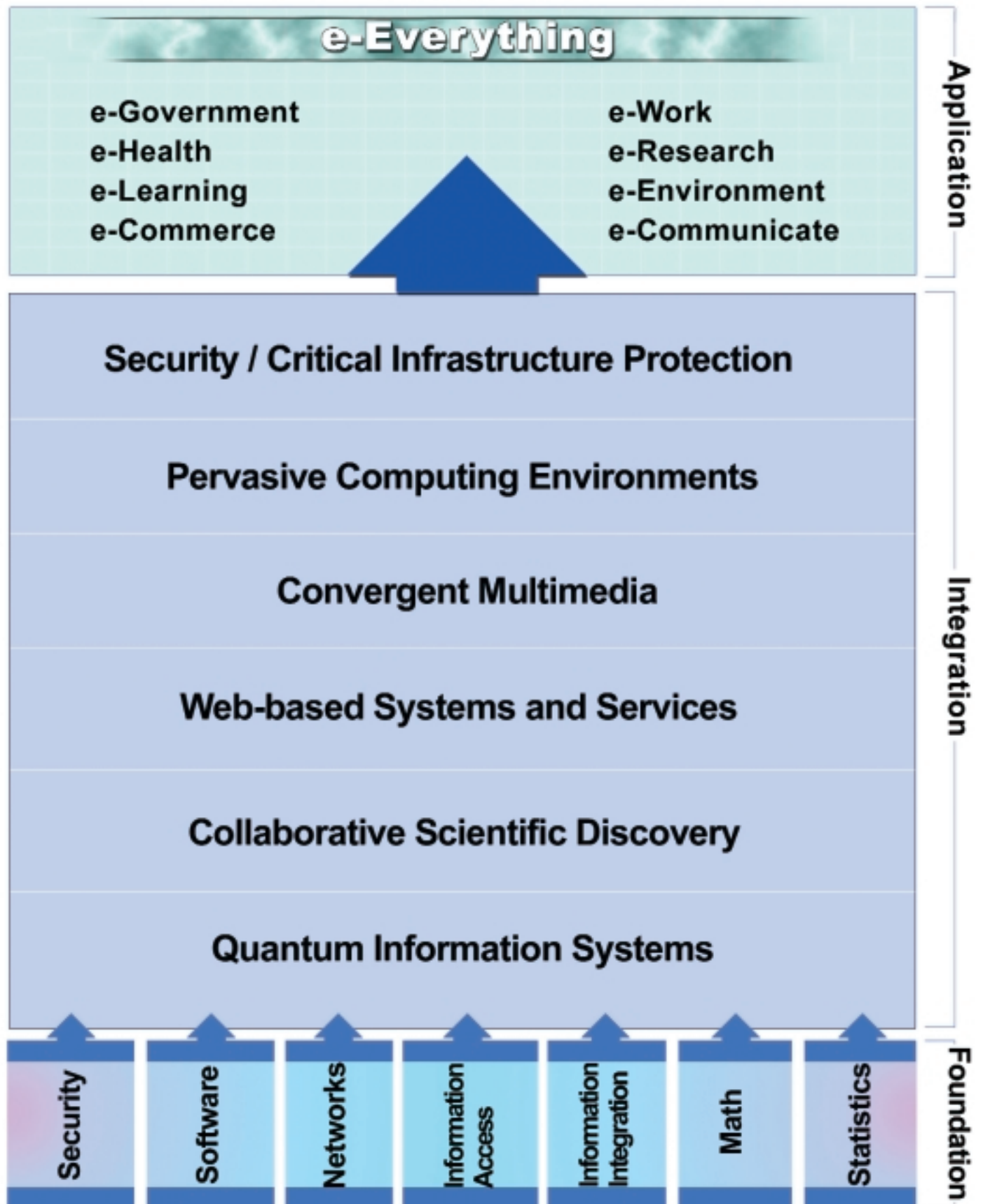
OUR CUSTOMERS

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

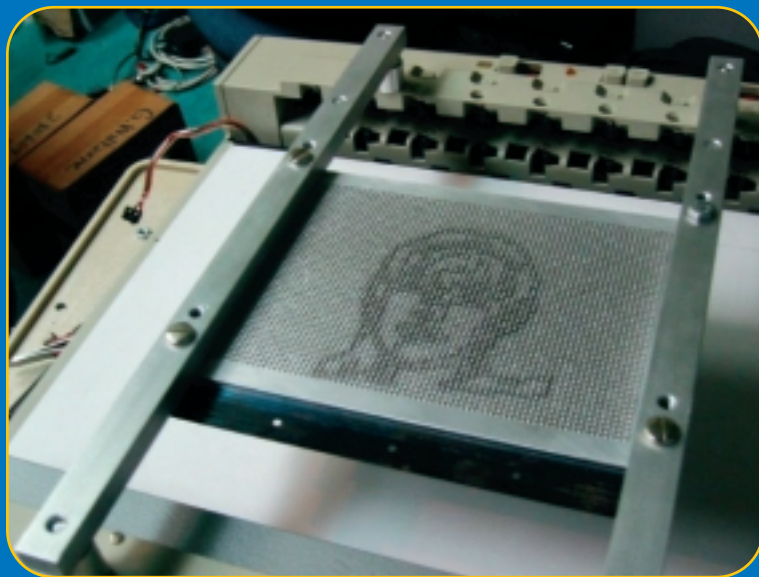
OUR RESEARCH PROGRAM

The following chart represents the ITL Research Blueprint, the framework by which we describe our research program. Our seven research divisions provide a crucial foundation in information technology measurements and standards, and these efforts are integrated into cross cutting areas such as critical infrastructure protection and pervasive computing. This research approach provides enabling technologies necessary to achieve the promise of all e-Applications.

ITL RESEARCH BLUEPRINT



ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM



A new refreshable tactile graphic display technology developed by ITL allows the blind and visually impaired to view images using the sense of touch. Estimated cost is a factor of twenty less than conventional technology.

FOUNDATION RESEARCH AREAS

SECURITY

Joan Hash and Alicia Clay discuss the success of the Small Business Computer Security Workshop series.



CRYPTOGRAPHIC STANDARDS AND APPLICATIONS

Our toolkit of secure cryptographic algorithm standards and standardized security techniques and protocols continued to grow in FY 2002. The Secretary of Commerce approved the Advanced Encryption Standard (AES) as Federal Information Processing Standard (FIPS) 197 in December 2001. The Keyed-Hash Message Authentication Code (HMAC) was approved as FIPS 198; HMAC tests are now available. We published the updated FIPS 180-2, Secure Hash Standard, in August. Other cryptographic FIPS are being updated to provide commensurate levels of security, including FIPS 186-2, Digital Signature Standard, where larger keys are needed for digital signatures. We published NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques; work continues on advanced modes. In November 2001, we conducted a workshop to develop a public key-based key management standard, as well as scheme and guideline documents for key management. We published a summary ITL Bulletin in September 2002 updating the progress of our cryptographic toolkit.

Through the NIST toolkit of standard algorithms, protocols, and techniques, ITL is enabling more efficient, secure, and interoperable information systems and electronic commerce. Government and industry will be able to build secure, interoperable applications with high-assurance

products that implement needed cryptographic security functionality. The website is <http://csrc.nist.gov/encryption/>

Our Public Key Infrastructure (PKI) work also advanced. We hosted the First Annual Public Key Infrastructure Research Workshop in April 2002; this workshop is expected to become an annual event. With the Federal Deposit Insurance Corporation and the Army Corps of Engineers, we developed a high-level Application Programming Interface (API) for PKI-enabled financial management systems; implementation of the API is in process. We supported the Federal PKI Steering Committee and subcommittees, which developed the Federal Bridge Certification Authority (FBCA); four agency PKIs have completed cross-certification with the FBCA, which is now operational. We completed a Secure/Multipurpose Internet Mail Extensions (S/MIME) profile and testing. Our Federal Directory Profile for PKI was revised based on empirical results. See <http://csrc.nist.gov/pki/>.

SECURITY MANAGEMENT AND GUIDELINES

For many years, ITL's Computer Security Division has been mandated by legislation to provide computer security standards and guidelines to federal agencies for protecting sensitive unclassified information in federal IT systems and networks. We issue computer security policy and management guidelines for federal agencies and support other federal agencies in their computer security program efforts. Our active outreach program provides assistance to government, industry, academia, and the public.

In FY 2002, we published guideline documents on the following topics: intrusion detection systems, risk management, active content and mobile code, security self-assessment, underlying technical models for IT systems, contingency planning, block cipher modes of operation, handling security patches, firewalls and firewall policy, telecommuting and broadband communications, interconnecting IT systems, and use of the common vulnerabilities and exposures (CVE) vulnerability naming scheme. Drafts are in process on additional security-related topics,

including security in procurements and certification and accreditation. We also published seven ITL Bulletins with a security focus. Our new Automated Security Self-Evaluation Tool, ASSET, version 1, became available online in June (<http://csrc.nist.gov/asset/>). Our Computer Security Expert Assist Team (CSEAT) provides automated information security program reviews of federal agencies upon request. CSEAT successfully completed a security review of the Indian Trust Management program within the Department of the Interior; more reviews are planned in FY 2003. Our Computer Security Resource Center is one of the most visited websites at NIST: <http://csrc.nist.gov>.

Outreach activities for federal agencies included hosting the federal computer security program managers forum, which held bi-monthly meetings in FY 2002 and sponsored two IT Security Metrics workshops for federal managers. The computer system security and privacy advisory board met four times in the year to identify emerging security issues and advise the NIST Director and the Secretary of Commerce on their findings. We established a Federal Practices Website (<http://csrc.nist.gov/fasp/>), an outgrowth of the Federal CIO Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection and security.

Our outreach to small- and medium-sized businesses expanded. In co-sponsorship with the Small Business Administration and the National Infrastructure Protection Center, we conducted six regional security meetings in Richmond, Virginia; Raleigh/Durham, North Carolina; Birmingham, Alabama; Washington, D.C.; San Francisco, California; and Chicago, Illinois. The website is <http://csrc.nist.gov/securebiz/index.html>.

SECURITY TESTING AND METRICS

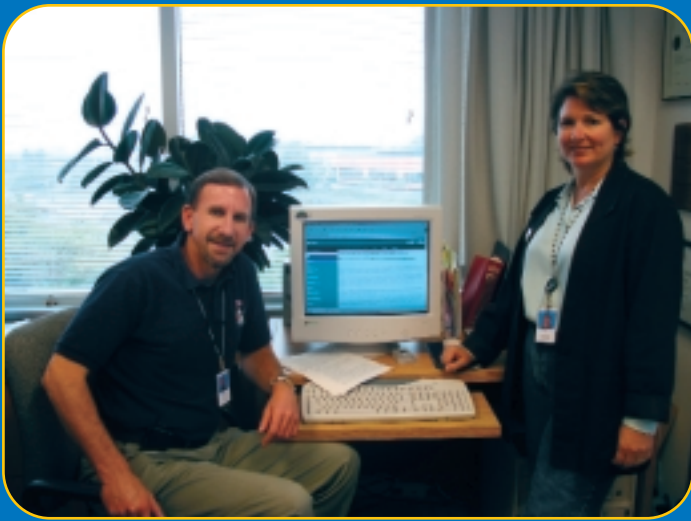
ITL strives to provide federal agencies, industry, and the public with a proven set of IT security services based upon sound testing methodologies and test metrics. Our security testing program includes cryptographic security testing via the Cryptographic Module Validation Program (CMVP) and the National Information Assurance Partnership (NIAP), which conducts testing using Common Criteria (CC) based specifications. Our testing-focused activities include the validation of cryptographic modules and cryptographic algorithm implementations, CC evaluation and validation programs, international recognition arrangements, testing laboratory accreditation, automated security testing and test suite development, industry forums, and education, training, and outreach programs.

The CMVP is a highly successful, internationally recognized program that to date has issued 257 validation certificates representing about 300 individual cryptographic modules from 69 IT vendors. In FY 2002, testing of modules began against FIPS 140-2, Security Requirements for Cryptographic Modules, which superseded the discontinued FIPS 140-1 in May; all modules entering our accredited laboratories are now validated under the updated FIPS 140-2 specifications. We completed the FIPS 140-2 Derived Test Requirements and a validation test tool in November 2001. We co-sponsored a second CMVP workshop in March. A sixth testing laboratory was accredited this year, the second Canadian laboratory to gain accreditation. Our Cryptographic Algorithm Validation System, including the AES Test Suite and DES/TDES enhancements, was released to the accredited CMVP testing laboratories in March. Also implemented was a CMVP cost recovery plan. To date, we have also validated 209 cryptographic algorithms, including AES, DES, TDES, Skipjack, SHA-1, and DSA. The website is <http://csrc.nist.gov/cryptval/>.

The National Information Assurance Partnership (NIAP), an alliance between NIST and the National Security Agency, continued to promote the development of a more secure IT infrastructure within the United States. The CC Evaluation and Security Program has tested 9 products



Summer Undergraduate Research Fellowship (SURF) students Amarpreet Cheema and Wendy Chou discuss their projects (cryptographic validation testing and a statistical test suite for random number generators) with advisor Larry Bassham.



*Ron Ross and Marianne Swanson review comments received on their document, **Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems**.*

and 12 protection profiles to date, for a total of 21 CC validations. The CC Smart Card Security Project, Phase II, is ongoing. We co-sponsored an IT security conference on continuity of operations at NIST in April 2002, and participated in May in the third International CC Conference held in Ottawa, Canada. At the conference, NIAP awarded nine CC certificates for successful evaluation of commercial, off-the-shelf (COTS) products and protection profiles against the Common Criteria for IT Security Evaluation (ISO/IEC 15408). The CC Recognition Arrangement was expanded to 15 nations, adding Sweden. The NIAP website is <http://niap.nist.gov/>.

SECURITY OF EMERGING TECHNOLOGIES

The mission of ITL's security research is to identify emerging technologies and conceive of new security solutions that will have a high impact on the critical information infrastructure; perform research and development on behalf of government and industry in the earliest stages of technology development through proof-of-concept, reference, and prototype implementations and demonstrations; and transfer new technologies to industry, produce new standards, develop tests, test methodologies, and assurance methods.

Example FY 2002 projects include access control and authorization management, the ICAT web-based Vulnerability Patch/Search database, the Government Smart Card Interoperability Specification, mobile device security, Internet Protocol security (IPsec) reference implementation and interoperability testing, and the administration of the critical infrastructure protection (CIP) grants program. RBAC FY 2002 technical accomplishments include the publication of the RBAC proposed standard (<http://csrc.nist.gov/rbac/>) as a reference model and functional requirements specification and an accompanying reader guide, and completion of an RBAC cost model and cost calculator. ITL RBAC research has been independently credited by the Research Triangle Institute (RTI) with saving industry \$295M and merited a 2002 Department of Commerce Gold Medal for three ITL scientists. We added and analyzed over 2,000 additional CVE vulnerability entries to our ICAT database, which now receives nearly 300K hits per month. We published the Government Smart Card Interoperability Specification, V2.0, (<http://smartcard.nist.gov/>) in June 2002, further promoting smart card device and application interoperability. The Smart Card Alliance stated, "The release of the Government Smart Card Interoperability Specification is a significant event in the smart card world as it is the first comprehensive effort to address the interoperability requirements of the enterprise market. It will become as important as Europay/Mastercard/Visa (EMV) specification is to the Payment market and Global System Mobile (GSM) specification is to the mobile telephony market."

We continued our research and prototype implementation to improve the security of handheld wireless devices. Research included adding new security features in the areas of: user authentication (through the use of biometric, smart card, and password technologies), security policy enforcement (based on the user's role, the environment of use, and the enterprise usage specification), and secure wireless policy delivery. Our IPsec effort continued in FY 2002 with the development of a Simple Network Management Protocol (SNMP) policy capability and by collaborating with IPsec vendors in the pursuit of large-scale IPsec and PKI-based virtual private networks (VPNs). This work is closely aligned with our advanced network research. We monitored progress on CIP grants awarded last year, which show promising preliminary results in wireless security, telecom security, electric power grid, intrusion detection systems, and security compilers. The website is http://csrc.nist.gov/focus_areas.html#research.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

SOFTWARE

ELECTRONIC COMMERCE

Electronic commerce (EC) solutions are being built using XML technologies as building blocks. Interest in conformance testing is growing, as indicated by increased conformance-related activities in industry consortia and working groups. Conformance tests improve implementations and the success of interoperability, which is critical. ITL's role is to improve the quality of XML-related software through the development of standards, conformance testing, and quality assurance practices.

In FY 2002, we led the conformance test development efforts for several World Wide Web Consortium (W3C) Working Groups, including the XML Core, Extensible Stylesheet Language/Formatting Object (XSL-FO), and Document Object Model (DOM). We developed and applied automated test generation techniques to effectively and efficiently produce tests for the various XML technologies. As a result of our efforts, the W3C has released the XML 1.0 (Second Edition) Conformance Test Suite. Additionally, we continued the development and release of conformance test suites for XML-FO, XML Schema, and DOM Levels 1 and 2. We initiated new conformance efforts for XInclude, Namespace, XML Protocol, and XML Query with W3C. As a result of our expertise, we co-founded and chair the W3C Quality Assurance (QA) Interest Group. We authored the QA Framework: Specification Guideline and contribute to the other QA Framework documents, i.e., Operational Guideline and Test Materials Guideline.

In a related project, we worked with the Organization for the Advancement of Structured Information Standards (OASIS) to develop a consistent test framework for all electronic business XML (ebXML) testing efforts. This framework was used to develop conformance tests for the ebXML

Registry and Messaging specifications. Messaging provides a method for exchanging electronic business transactions and registries to allow for the discovery and retrieval of XML-related documents. We finalized the Registry specifications (v2) and progressed it as an OASIS Standard. Additionally, we developed proof of concept registry prototypes for the General Services Administration (GSA) and the Environmental Protection Agency (EPA). We chaired the OASIS Conformance Technical Committee and we completed the GSA Standards Roadmap prototype, which is being used as the model for an IT standards roadmap for healthcare.



Carmelo Montanez-Rivera, Richard Rivello, Sandra Martinez, and John Tebbutt help make electronic commerce a reality by developing tests for the family of XML technologies.

Another ITL project is the development of standards and tests required for the success of Interactive TV (ITV). For the Society of Motion Picture and Television Engineers (SMPTE), we made significant contributions to the Declarative Data Essence (DDE) specifications. We authored several sections and produced reference



Doug White and Mark Rose (seated) help the law enforcement community apprehend criminals and terrorists by developing reference data and tests for computer forensics.

applications illustrating DDE-1 content for the DDE-1 Engineering Guide; DDE-1 is expected to become the first international ITV standard (ISO/IEC). We also developed a Digital TV (DTV) Application Software Environment (DASE) Trigger Abstract Test Suite. We completed our ITV project at the end of FY 2002.

Our support of the federal CIO Council continued. We assisted the XML Working Group of the CIO Council by chairing their registry subcommittee and hosting a registry where federal agencies can learn about how to use XML registries. The website is <http://www.itl.nist.gov/div897/>.

HEALTHCARE

Although the healthcare industry is one of the major industries in the United States, it has been one of the slowest to embrace information technologies in its operations. We are working with the healthcare industry, government agencies, and academia to improve the quality of healthcare, reduce costs, and provide essential services through the use of information technology. With Advanced Technology Program support, we provide the technical leadership in integrating healthcare standards into emerging e-commerce frameworks. In August, we held the first in a series of workshops aimed at understanding the issues involved in the effective use of IT for healthcare and related fields. The workshop, "Information Technologies for

Healthcare: Barriers to Implementation," focused on identifying the key issues and barriers to improve quality and productivity. We published a workshop report and established a website to inform the public of our efforts as well as to facilitate a continued dialogue among interested parties. We have joined the Health Level Seven (HL7) Consortium and actively participate in several committees, including the Conformance group. We developed a concept paper on Healthcare Information Standards and Testing that discussed options for analyzing, defining, and organizing appropriate standards for the healthcare community and the issues surrounding conformance testing. The paper has been used to stimulate discussion and foster opportunities for collaboration between the healthcare community and NIST. As a result of the concept paper and discussions with members of the community, we have begun work on the development of a healthcare standards roadmap, which will provide a set of web services and infrastructure for establishing, populating, searching, maintaining, and administering healthcare standards information.

Our work in Health Information Systems continued. The Department of Veterans Affairs (VA) is a primary federal customer. As the deployment of the Enterprise Single Sign-On (ESSO) to all VA hospitals proceeds, we modified VA applications and ESSO, and assisted in the development of diagnostic and administrative tools for ESSO. We developed a v2 reference implementation of the Inter-Organizational Role Based Access Control (IORBAC) with Resource Access Decision (RAD) functionality. See http://www.itl.nist.gov/div897/docs/healthcare_information_systems.html.

COMPUTER FORENSICS

Since the tragedy of September 11, 2001, ITL's work in computer forensics has taken on added significance and impetus. Sound computer forensics practices are a key to finding and delivering court-permissible evidence when computers are used in the commission of a crime. Our program has two components: the National Software Reference Library (NSRL) and Computer Forensics Tool Testing (CFTT).

Investigators often spend hundreds of hours looking at digital evidence seized in the course of a criminal investigation. Our NSRL eliminates much of this labor-intensive work by automation. The NSRL is a reference data set of file signatures (hashes) of commercial off-the-shelf files,

which can be used during examination of digital evidence to identify pertinent files and eliminate others. One computer may have 5,000-75,000 files. The NSRL data set can eliminate 40-95 percent of commercial, off-the-shelf (COTS) files from examination and save hundreds of staff-hours. In FY 2002, we continued to develop and populate the NSRL, which now contains over 8,000,000 file signatures. We issued the first release in October 2001 as NIST Special Database 28 and updated it quarterly. The NSRL has been incorporated into several computer forensic tools and the National Archives and Records Administration has asked to work with us to use the NSRL to support electronic records management.

The goal of our CFTT project is to provide a measure of assurance that the tools used in computer forensics investigations produce accurate results. This is accomplished by developing specifications and test methods. In FY 2002, we finalized the specification for disk imaging tools and released a draft specification and test assertions for hard disk write blocking. We released software tools and methodology for testing disk imaging software. The National Institute of Justice issued a disk imaging report based on our methodology. We also released a general methodology paper, developed an extensive peer review process, and established partnerships with the digital evidence community. An ITL researcher serves as an editor for the new Journal of Digital Evidence. The websites are <http://www.nsrl.nist.gov/> and <http://www.cftt.nist.gov/>.

RESEARCH TO IMPROVE SOFTWARE TESTING

ITL develops tools and techniques to improve the development of specifications, software tests, and software quality. The national annual cost of an inadequate infrastructure for software testing is estimated to range from \$22.2 to \$59.5 billion. Testing activities account for 30 to 90 percent of software development costs. In addition, software testing is time-consuming, labor-intensive, not comprehensive, and difficult to measure. Poor software quality also contributes

to security incidents. Our automatic test generation (ATG) project provides a method for automatically generating tests from formal specifications.

In FY 2002, we advanced the development of XML-based formal model intermediate representation with the Simulink/Stateflow Intermediate Representation (SSIR) Group. Consisting of NIST, Ford Motor Company, Carnegie Mellon University, General Electric, Vanderbilt, and TriPacific, the SSIR Group seeks to standardize an intermediate representation of formal models. We assisted the commercialization of the ATG method with the Ford Motor Company and New Eagle Software. We continued feasibility studies with the Argus Systems Group on a secure computer operating system and with Northrop Grumman on fighter radar computers.



William Majurski, Leonard Gebase, and Mary Laamanen apply emerging e-commerce standards and technologies to the health-care industry and the Department of Veteran Affairs.

Our work on Object Oriented (OO) Component Testing continued. The project (formerly Software Testing by Statistical Methods) addresses the development of new methods for software testing based on stochastic processes and metrics. Its objectives are to improve software quality, reduce testing costs, and develop reliability estimates that software correctly adheres to its specification. Our approach is to develop a new conformance testing methodology for OO environments and to concentrate on component integration. See <http://www.itl.nist.gov/div897/>.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

NETWORKS

AGILE SWITCHING INFRASTRUCTURES

ITL works with industry to accelerate the development of integrated, agile switching infrastructures. The main focus of the project is on integrated control planes for optical switched networks, dynamic control algorithms for traffic engineering, and protection and restoration. Current efforts focus on the modeling and analysis of signaling protocols and optical network protection and restoration mechanisms, the development of simulation tools, and the creation of a testbed experimenter's toolkit.

In FY 2002, we developed two research tools: a Multi-Protocol Label Switching (MPLS)/optical network simulator (NIST GLASS) and a testbed experimenter's

toolkit, MPLS on Linux for Traffic Engineering (NIST Switch). We also published many papers on optical network fault detection, protection, and restoration. We worked with the Internet Engineering Task Force (IETF) and the Optical Internetworking Forum (OIF) to develop technical specifications for an integrated control plane combining optical and Internet switching and provided modeling and analysis tools to the research community. Next year we will focus on standards for optical network protection and restoration, and technologies for optical burst switching (OBS). Our contributions of rapid prototypes, and modeling and analysis tools benefit industry and academic researchers working on the next-generation optical Internet. The website is http://w3.antd.nist.gov/agile_switch.shtml.



Leonard Miller, Camillo Gentile, and Luke Klein-Berndt develop protocols for wireless ad hoc networks.

INTERNET INFRASTRUCTURE PROTECTION

ITL strives to improve the scalability, performance, and interoperability of Internet security systems and to expedite the development of Internet infrastructure protection technologies. Our technical approach is to lead the effort within the IETF to complete the Domain Name System Security (DNS SEC) standardization process. Our modeling, analysis, and testing tools help to evaluate emerging Internet key management protocols. The integration between quantum key distribution and Internet security protocols is another area of interest.



Kevin Mills, Scott Rose, Doug Montgomery, Chris Dabrowski, and Steve Quirolgico work on service discovery protocols for networking for pervasive computing.

In FY2002, we contributed revised IETF specifications for DNS SEC protocols. Our Advanced Encryption Standard (AES) is being incorporated into Internet security standards. We sponsored a workshop for federal agencies on the deployment of DNS SEC. We published a performance/interoperability analysis of emerging DNS SEC protocols. We contributed modeling and analysis results to the IETF efforts to design new key management systems. We also developed extensions to IPsec/IKE protocols to exploit one-time keypads from quantum key distribution. Our work with the IETF results in increased Internet security at a lower cost. The website is <http://w3.antd.nist.gov/iipp.shtml>.

INTERNET TELEPHONY

ITL facilitates the development of improved Voice over Internet Protocol (IP) (VoIP) transport mechanisms and expedites the development of new, programmable telephony signaling services. Our approach is threefold. We are researching the approaches to resource control for emerging Internet telephony service creation architectures. We also research the application of Internet telephony signaling protocols to presence/location

tracking and device control in pervasive computing environments. Lastly, we deliver rapid prototypes, and test and instrumentation tools to the IP telephony industry.

In FY 2002, we assumed leadership of the Java™/JAIN™ Session Initiation Protocol (SIP) specifications. SIP is an HTTP-like signaling protocol used to set up and manage media sessions, such as telephone calls, Instant Messaging, video, or games. It is an enabling technology for new media services. Customers of this work include platform vendors, service vendors, service providers, and industry groups. We completed NIST-SIP 1.0, our prototype research platform and associated test tools. We delivered research prototypes and a test system for the emerging JAIN/SIP protocols to thousands of early adopters of the technology. We also designed and evaluated techniques for resource control in fully programmable service creation environments.

ITL's contributions are improving the quality and expanding the scope of the next generation Internet telephony signaling technology. We are helping industry to design new capabilities and uses for Internet telephony signaling protocols and delivering research platforms

and test systems for their use. Our work enables the emergence of new markets for multi-modal Internet applications. The website is
http://w3.antd.nist.gov/it_voip.shtml.

WIRELESS AD HOC NETWORKS

The goal of this ITL project is to facilitate the development of technology and standards for wireless ad hoc networks (WANETs). A WANET is a collection of stationary/mobile nodes with wireless communication and possible multi-sensory capabilities. Key features include the lack of need for any prior infrastructure, self-organization, and adaptation to varying topology. These networks have commercial applications, such as congestion mitigation in hot spots, guerilla networks, and healthcare facilities. Some are mission-oriented networks, including first responder communications and networking, battlefield deployment of military forces, and smart sensor networks.

Our approach is to develop metrics and measure the performance of various WANET protocols proposed to the Internet Engineering Task Force (IETF), thereby facilitating the IETF standardization process. We are

also developing simulation models of popular WANET protocols and developing a WANET hardware testbed to complement our analytical and simulation work. In FY 2002, we evaluated self-organization algorithms for sensor networks. We developed and implemented a prototype for enhancements to ad hoc network routing algorithms. We developed testbeds and conducted experiments for video streaming over wireless ad hoc networks. We also helped the IETF to enhance the AODV protocol (the leading on-demand ad hoc routing protocol). We significantly improved the 802.11 OPNET® model and developed video transmission schemes for first responder ad hoc networks. Our work was documented in more than 20 papers presented at professional conferences.

ITL's research and standardization efforts have significant impact on future applications, especially military and first responder applications, of wireless ad hoc networks. Researchers in industry and academia also use our metrics and performance measurements to advance the technology. The website is
http://w3.antd.nist.gov/wahn_home.shtml.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

INFORMATION ACCESS

HUMAN LANGUAGE TECHNOLOGY

Within the broad field of human language technology, ITL develops and applies metrics and testing to advance the state of the art of human language processing, including speech recognition, speaker recognition, spoken language understanding, search, retrieval, filtering of text-based information, and other advanced text processing techniques such as summarization, extraction, and question answering. Our work is organized into five projects: TREC, ACQUAINT, TIDES, ACE, and Speech Processing.

Our Text REtrieval Conference (TREC) series, initiated in 1992, 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, a means to accelerate technology transfer, and an incubator for new research areas. We co-sponsored with the Defense Advanced Research Projects Agency (DARPA) TREC-2001, with 87 groups participating from 21 countries; the conference included a web task, a question answering task, a filtering task, and a cross-language retrieval task. We published the proceedings in paper and online. We initiated the planning for TREC-2002, procuring new data, designing an XML task, and defining a new novelty track. The goal of our related ACQUAINT program is to move the state of the art of question answering to the full range of complex questions asked by humans. At the kickoff meeting in December 2001, we presented a draft plan for the overall evaluation, worked with the research community to define a set of pilot evaluation projects for eight advanced question types, and obtained three gigabytes of new data for use in AQUAINT.



Mike Garriss and Steve Wood are shown developing new measurement standards for fingerprint biometrics as part of the USA Patriot Act and Enhanced Border Security Act.

DARPA's TIDES (Translingual Information Detection, Extraction, and Summarization) program addresses the problem of finding and interpreting needed information quickly and effectively regardless of language. Sponsored by TIDES, the Document Understanding Conference (DUC) series is run by ITL to further progress in summarization and enable researchers to participate in large-scale experiments. For DUC 2002, held in Philadelphia in July, we revised evaluation protocols to include a specific set of questions to evaluate summary quality and devised a new metric called length-adjusted coverage. We built an additional 60 sets of documents and summaries, and created multi-document extracts at the 200- and 400-word levels. For the TIDES Topic Detection and Tracking (DTD) project, we hosted the TDT 2001 evaluation, analyzed the evaluation results, and presented our work.



Audrey Le and Gregory Sanders consult with Christophe Laprun on how ATLAS (Architecture and Tools for Linguistic Analysis Systems) can be used in the next generation speech recognition evaluation

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 2002, we supported evaluations of extracting content from these media in February and September. We further developed evaluation measures and provided detailed analysis of results for the Entity Detection and Tracking (EDT), Cross-Document EDT, and the Relation Detection and Characterization (RDC) tasks. We oversaw the annotation of ACE corpora for EDT and RDC training and evaluation test sets. Additionally, we are creating links between the ACE and Evidence Extraction and Link Detection (EELD) communities with combined evaluations.

Our speech processing projects help to advance the state of the art in speech recognition and understanding for applications in human-computer interaction and access to spoken information. Corpora collected from the Automatic Meeting Transcription project is made available to industry through the Linguistic Data Consortium (LDC). Evaluation tools are available at http://www.nist.gov/speech/test_beds/mr_proj/. In FY 2002, we completed the equipment/software infrastructure for data collection, including 200

microphones and five video cameras. We hosted a Meeting Transcription Workshop and created a cross-site effort in data pooling. We used NIST and multi-site data for the Rich Transcription (RT-02) evaluation in April 2002. We designed an ontology of meeting types, chose scenarios, built a website, and recruited subjects. Lastly, we collected hours of various types of meetings, created an extensive log, and provided the corpus to LDC for transcription and distribution.

For the DARPA Effective, Affordable, Reusable Speech-to-Text (EARS) program, we provide accuracy measurements of core speech-to-text and metadata recognition. In FY 2002, we conducted preliminary metadata experiments to determine target set and feasibility. We implemented an evaluation incorporating news broadcasts, telephone conversations, and meeting speech for speech-to-text transcription and speaker segmentation with a variety of test conditions. We organized and ran the RT-02 Workshop and began the development of the evaluation infrastructure for RT-03.

Our Speaker Recognition work progressed. We conducted the 2002 NIST evaluation with a record 25 participating sites from five continents. We included a new multi-modal test. Expanded to three days, the 2002 Speaker Recognition Workshop was held in May in Virginia.

ITL's human language technology programs contribute to improved Internet and intranet information retrieval performance in the next generation of search engines. The website is <http://www.itl.nist.gov/iad/programs.html#Human>.

INTERACTION AMONG USERS AND INFORMATION

To improve the usability of interactive systems, ITL is providing metrics, standards, and test methodologies by developing standard usability reporting formats, new approaches and benchmarks to support usability testing (especially for the web), approaches for accessibility testing, and advanced user interface prototypes. Our work focuses on usability engineering and IT accessibility.

Our Web Metrics work advanced in FY 2002. We redesigned our Web Category Analysis Tool (WebCAT) software, which had 1,500 downloads from our website. We optimized our Web Variable Instrumenter Program (WebVIP) software and redesigned it for added reliability. We enhanced the Framework for Logging Usability Data (FLUD), a file format and parser for representation of user interaction logs. We also chaired a workshop for the W3C usability interest group. In our Industry USability Reporting (IUSR) project, our Common Industry Format (CIF) was adopted as a national standard (ANSI/ NCITS 354) in November 2001; the international standardization of CIF is moving forward. To create benchmark test data for web usability evaluation methods, we analyzed results of the pilot studies on CIF Testing, Evaluation, and Reporting (CIFter). Results were published, and a workshop is planned for participants in the CIFter I evaluation. To ensure IT accessibility, we provided technical guidance to the Objective Measures Project of the Section 508 Accessibility Forum. We also participated in the NCITS V2 Technical Committee, which is developing Alternative Interface Access Protocols that will allow alternative interfaces for people with disabilities. The website is <http://www.itl.nist.gov/iad/programs.html#Users>.

website for MPEG-7 reference software and documentation, chaired and participated in various MPEG-7 committees, helped to establish an MPEG-7 Alliance industry forum, worked with industry to define MPEG-7 interoperability and profiling, and developed a web-based MPEG-7 system to validate MPEG-7 data structures.

The goal of our TREC Video Retrieval Task is to foster research in content-based retrieval from digital video. Our approach is to create a publicly available test collection of digital video for use by the research community. In FY 2002, we presented TREC-2001 results at a workshop and completed the guidelines for the 2002 Video Track. We selected 70 hours of video data hosted by the Internet Archive and, working with industry partners, defined ten features for the extraction task. We are also developing required topics and evaluation software for automatic and human assessment of task results. Our visualization and virtual reality for manufacturing project progressed. We played a key role in organizing the Web3D 2002 Conference, improved access to raw anthropometric subject data, incorporated a VRML/X3D translator into the prime X3D tool, and released the first version of the NIST CAESAR Viewer, a web-based 3D body visualization. The website is <http://www.itl.nist.gov/iad/programs.html#Multi>.

MULTIMEDIA TECHNOLOGY

To advance technologies for accessing and using multimedia information, including multimedia searching and filtering, ITL's approach is to actively participate in standards development, testing of content-based retrieval from digital video, and visualization and virtual reality for manufacturing.

Through leadership positions on standards committees (MPEG, JPEG, Web3D), we continue to advance multimedia standards. In FY 2002, we planned, coordinated and presided over the U.S. NCITS/L3 meetings. As the chair of this national standards committee, we coordinated and participated in MPEG and JPEG international meetings and hosted an international MPEG meeting in Virginia. We hosted an online MPEG data repository and management information system. In related work, we develop measurement methods for the evaluation of multimedia metadata (MPEG-7) for the purpose of content-based multimedia retrieval. To advance this technology, we created an MPEG-7 data repository



Karen Marshall directs indoor photo shots while Stan Janet readies the camera for outdoor images taken of NIST volunteers for the NIST Human ID Image Collection, used to develop metrics for evaluating face recognition systems.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

INFORMATION INTEGRATION



Alexei Nikolaev, Charles Fenimore, and John Roberts view the results of NIST-developed tests for image quality of digital content for various display platforms.

In FY 2002, we completed the first phase of disc reliability studies for CD/DVD, looking at temperature, humidity, and photo degradation with a microscopic image observer. For the NIST/HDSA Data Preservation Laboratory, we installed test equipment to evaluate the interoperability of storage devices and media. We used the NIST CD Compliance Test software (<http://www.itl.nist.gov/div895/products.html>) to check compliance with the Optical Storage Technology Association (OSTA) MultiRead specification; publications on this work are in process. In June, we co-sponsored with the DVD Association (DVDA) the NIST DVD 2002 Conference for industry and government, with a focus on media and player standards and interoperability, DVD authoring, and data preservation. We also serve on the National Digital Strategy Advisory Board at the Library of Congress. This effort is to develop a long-term national strategy to preserve the nation's born-digital artifacts. The website is <http://www.itl.nist.gov/div895/isis/projects/datastorage-project.html>.

DIGITAL CONTENT STORAGE: DATA PRESERVATION AND OPTICAL DISC STANDARDS

In response to the needs of industry for uniform and reliable, writable disc media, ITL is developing standards, test methodologies, and guidelines to promote interoperability for disc media, reliability, and preservation of data. Many disc formats (five for DVD) are not interoperable for current disc drives. Guidelines and standards are lacking. Our approach is to systematically study recordable disc media reliability under numerous conditions and develop software to promote and check for disc drive interoperability. We also work closely with the High Density Storage Association (HDSA), a non-profit organization comprised of manufacturers, resellers, individuals, and end-users interested in high-capacity storage technologies and products, and in their cross-platform interoperability.

DIGITAL CONTENT MANIFESTATION: BRAILLE DISPLAYS AND IMAGE QUALITY

ITL is developing guidelines and standards for content manifestation to ensure fidelity and quality of image presentation for various formats, platforms, and end-users. To achieve a superior quality of a digitized image file, the issues of file compression and lack of open standards for file quality manifestation must be addressed. Our approach is to develop test corpora suites in cooperation with the Motion Picture Experts Group (MPEG) and the Society of Motion Picture and Television Engineers (SMPTE) and to distribute the test suites to end-users, projector manufacturers, and digital test laboratories. In conjunction with our previous eBook work, NIST is also developing prototype, low-cost, mechanical Braille displays to place digital content in the hands of the blind community.

Our Image Quality Laboratory provides the research environment necessary to develop image quality measurement tools, test materials, and procedures, and to disseminate the research test corpora to industry. In FY 2002, we equipped our laboratory to conduct image quality studies. We developed an Image Comparator Tool, which demonstrates the NIST Just Noticeable Difference (JND)/Discrete Cosine Transform (DCT) metric. JND-DCT is a computed image quality metric designed to measure the difference between two images as perceived by a human viewer. The tool is available at <http://www.itl.nist.gov/div895/products.html>. We also developed digital content test tools and standard video evaluation materials. Our support of MPEG and SMPTE standards development activities continued. The website is <http://www.itl.nist.gov/div895/isis/projects/digitalcinemaproject.html>. We also developed a tactile graphics display that manifests pictures in pin-by-pin two-dimensional format for blind users to receive graphical information. The National Federation for the Blind will field test the NIST device and this information will be useful for third parties who plan to commercialize this NIST technology. More information is available at <http://www.itl.nist.gov/div895/isis/projects/brailleproject.html>.

DIGITAL CONTENT PACKAGING: FILE FORMATS

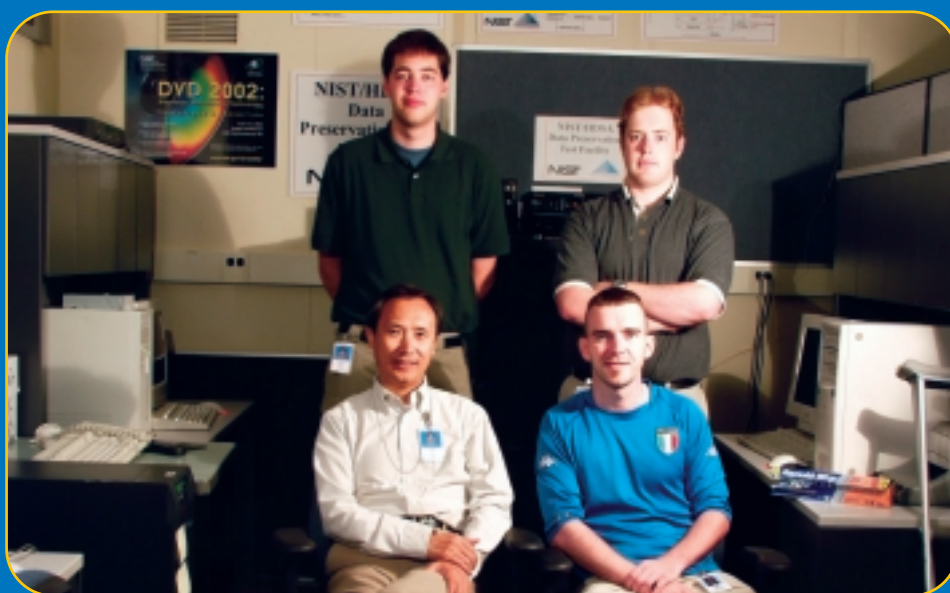
ITL's goal is to develop interoperability guidelines for digital content types, their use and scalability. We are defining the scope of content types to examine (video, film, text, pictures, audio) and developing an inventory of digital object types. We can then evaluate the sensitivity of various content types to media-specific failure mechanisms. Critical features are defined in terms of cost, performance requirements, and usage for content types.

In FY 2002, we completed our file format inventory and published results in a content type matrix. We conducted file format/temporal studies to detect and observe the time-dependent properties of displays that affect image quality and to correlate these properties with the presentation of different images and file formats.

In January 2002, we presented this work at a technical conference. We completed our Advanced Technology Program eBook File Format research; software is in development to allow any image format to be displayed on the NIST-developed tactile graphic display. To assess the feasibility of transferring scientific, technical, and medical documents to commercial platforms, we continued testing file formats for eBooks. We developed test corpora to evaluate formatting and to test device compliance to the Open eBook (OEB) specification. We developed an OEB Windows® Browser for a Windows® platform and made it available on the web. To date over 40 downloads of the OEB compliant browser for Linux have been made. More than 350 people attended our annual Electronic Book Conference and Show in Washington, D.C., in November 2001. The website is <http://www.itl.nist.gov/div895/isis/projects/ebookproject.html>.

DIGITAL CONTENT TRANSFER AND DELIVERY: DTV

ITL is developing metrics and guidelines for architectures ensuring the efficient delivery and transport of digital content. Our support of the digital TV industry continued in FY 2002. The Application Software Environment (DASE)-1 Specification was approved as a Candidate Standard. DASE is the North America middle-



John Costello (left standing), Sean Ginevan (standing), Xiao Tang (left seated) and Oliver Slattery are developing interoperability tests for high-density storage systems.



Xiao Tang (standing), Jian Zheng, and Fred Byers examine results of tests on the lifetime of DVDs.

DIGITAL CONTENT ENCAPSULATION: RIGHTS MANAGEMENT

ITL is developing interoperable open standards, guidelines, and specifications for rights management of digital content. While market progress on trust issues has been slow, the need remains high. Problems arise because the Internet cannot vouch for participants, a major inhibition to e-commerce. The issues are identity authentication, agreement assurance, and privacy. ITL's trust management project addresses these barriers.

Building upon our Financial Agent Secure Transaction (FAST) assurance framework, we collaborated with NIST's Electronics and Electrical

ware standard for broadcast interactive television. NIST and the DASE specialist group are developing these standards in advance of widespread use of digital television technology. We completed the DASE-1 Prototype Implementation, which provides application developers and consumer electronic manufacturers an application development environment and a basis for an interoperable Digital TV receiver implementation. We released the reference implementation to the public (<http://www.dase.nist.gov>), along with demo applications, the Advanced Television System Committee (ATSC)/MPEG parser, and documentation; the website has received over 5,000 hits to date. The prototype implementation provides the experimental environment needed to shape future commercial interactive Digital TV. Also under construction is a robust quantum communications testbed that will enable explorations of quantum information transmission. The website is <http://www.itl.nist.gov/div895/cmr/dase/index.html>.

Engineering Laboratory and the IPC (Electronics Interconnection Industry consortium) to apply the FAST model via existing Internet client-server technology and a legacy database. This model provides referral on identity, capability (products and services), trust, and reputation. In FY 2002, we completed a flexible, modular, server/portal mechanism for trust management. We compiled an inventory of digital rights management (DRM) standards and sponsored a workshop on DRM interoperability and standards. We analyzed authentication architectures and formats, and defined the compatibility of biometric data for content and devices. We served as a technical co-sponsor for the IEEE 4th International Workshop on Networked Appliances (IWNA-4) held at NIST. Our assurance and trust mechanism for Internet commerce for manufacturing will create new and expanded opportunities for small business in the electronic marketplace. The website is <http://www.itl.nist.gov/div895/cmr/ecom/index.html>.

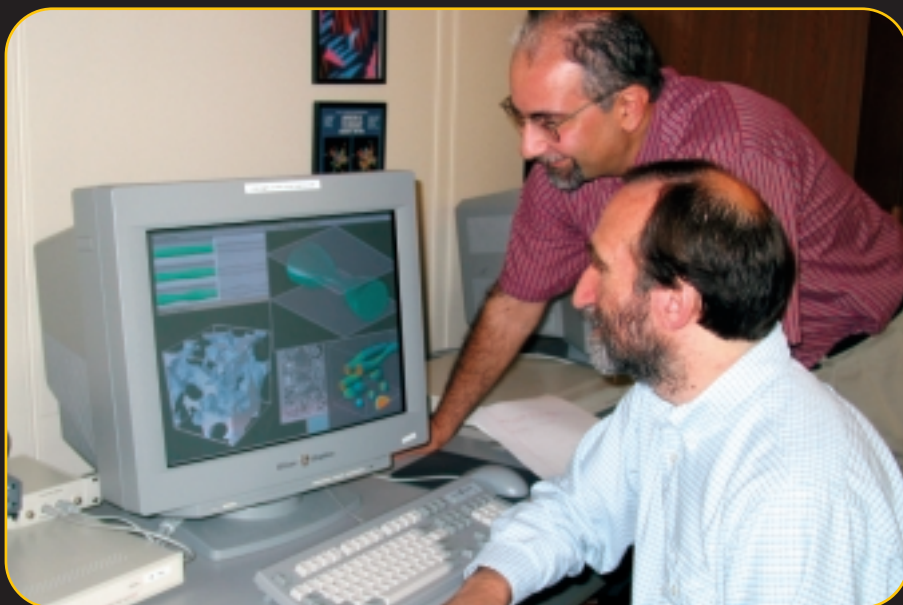
ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

MATHEMATICS

APPLIED MATHEMATICS

ITL's applied mathematics program focuses on the development of mathematical models, methods, and tools applicable to problems of national interest. Through extensive collaboration and consulting with NIST scientists, we help to improve the quality of NIST research via the application of state-of-the-art mathematical and computational methods. In addition, interactions with other federal agencies and industry partners ensure the widespread benefit from our work. The diverse application areas in which we work include atomic physics, bioinformatics, electromagnetics, materials science, manufacturing, and construction engineering. To these we bring expertise and develop new tools in ordinary and partial differential equations, continuum mechanics, nonlinear dynamics, numerical analysis, mathematical optimization, deconvolution, discrete mathematics, computational geometry, Monte Carlo methods, and data mining.

Our contributions to NIST's research program in FY 2002 are widespread. For NIST's Electronics and Electrical Engineering Laboratory (EEEL), we developed data correction methods and software for antenna quiet zone imaging. We also developed lattice sum techniques for computing band-gap diagrams for arbitrary two-dimensional photonic crystals and implemented these in software. For the Materials Science and Engineering Laboratory (MSEL), we developed a diffuse-interface model for electrodeposition coupling phase change and electrolytic reaction. For the Chemical Science and Technology (CSTL) Laboratory and the



John Hagedorn (seated) collaborates with Nicos Martys of the NIST Building and Fire Research Laboratory, applying methods of parallel computing and scientific visualization to improve the performance of the Lattice Boltzman method for the modeling of fluid flow in complex geometries.

Manufacturing Engineering Laboratory (MEL), we deployed our real-time blind deconvolution method to the sharpening of scanning electron microscope imagery. With NIST and industry partners, we are modeling high-speed milling to fulfill the measurements and standards needs of U.S. discrete parts manufacturers. In particular, we developed analytical models of coupled tool-assembly dynamical behavior to optimize tool design and reduce chatter. Our bioinformatics effort with NIST's CSTL and the National Institutes of Health involves applying optimization techniques, the Markov theory of random processes, and parallel computing to the challenging problem of aligning multiple protein sequences with gaps. With the Building and Fire Research Laboratory (BFRL), we made significant progress in the deconvolution of laser radar imagery for application in construction site management.



Isabel Beichl and NRC Research Associate David Song are working to understand the potential advantages and limitations of proposed quantum-based computers.

In addition, we continued our development of novel techniques and tools of wide application. We released a three-dimensional version of the Object-Oriented MicroMagnetic Framework (OOMMF), our widely used software for micromagnetics modeling. We improved the Object-Oriented Finite (OOF), our software tool for analyzing real material microstructures, developing new facilities for automatic grain boundary detection and mesh refinement. Implementation of OOF2, which will be capable of handling a much wider range of physical situations, is well under way. We also developed new Monte Carlo techniques for estimating independent sets in graphs, a problem arising in multiple contexts, from the study of communications network reliability to thermodynamics models. The website is <http://math.nist.gov/mcsdl/>.

DIGITAL LIBRARY OF MATHEMATICAL FUNCTIONS

The DLMF, now under development at NIST, is an interactive, web-based compendium on the special functions of applied mathematics. Such functions are basic tools in mathematical and computational modeling in many disciplines. Examples are Bessel functions, elliptic integrals and functions, the classical orthogonal polynomials, Heun functions, Painleve transcendents, and q-series. The core of the DLMF is a database of

mathematical properties compiled by some 40 external experts. ITL is coordinating and editing the database, and developing techniques for its effective online presentation. Components of the latter include semantic mathematical markup, interactive web-based graphics, search in mathematical databases, metadata, bibliographic links, and links to software. When completed, the DLMF will provide standardized notations, definitions and properties for special functions, with online traceability to NIST.

In FY 2002, working under the supervision of the NIST editors, most of the external authors completed acceptable drafts of their chapters. We generated some 100 visualizations, developed a prototype search engine, and constructed a seven-chapter prototype. We co-organized a two-week workshop on Special Functions in the Digital Age held at the Institute for Mathematics and Its Applications at the University of Minnesota in which many DLMF editors and authors participated. Next year we expect to complete the validation of chapters by external experts, produce a complete draft of the website, and contract for the printed version of the DLMF. The website is <http://dlmf.nist.gov/>.

HIGH PERFORMANCE COMPUTING AND VISUALIZATION

The need for higher fidelity models incorporating more complex physics often leads to computational problems that far exceed the capacity of current desktop workstations. Parallel computing techniques can be used to extend the computational power available on the desktop. ITL develops tools and techniques for high performance parallel and distributed computing, and collaborates with NIST scientists and engineers to apply these to problems of critical interest. High performance simulations, as well as emerging combinatorial experimental techniques, can yield massive amounts of data. Carefully designed scientific visualization methods and data mining techniques are needed to understand such data. ITL develops facilities and tools of this type, and collaborates with NIST scientists and engineers to apply them. Current applications include modeling of nanostructures, flow in porous media, solidification of metal alloys, and atomic physics.

In FY 2002, we expanded our Reconfigurable Advanced Visualization Environment (RAVE) immersive visualization facility to two 8 by 8 foot screens arranged at right angles, and developed new tools to ease its use. The facility now sees widespread use. We demonstrated the promise of virtual measurement systems by achieving the most accurate computation to date of the ground state of neutral helium. With CSTL, we produced a parallel version of the popular FEFF x-ray absorption spectroscopy software, providing a 20-fold speedup for such computations on workstation clusters. For MSEL, we created a parallel three-dimensional phase-field solidification simulator. We also developed parallel computing techniques and visualizations for studies of fluids, suspensions, and elasticity for the Virtual Cement and the Concrete Testing Laboratory in collaboration with BFRL. The website is <http://math.nist.gov/mcsd/savg/>.

MATHEMATICAL SOFTWARE

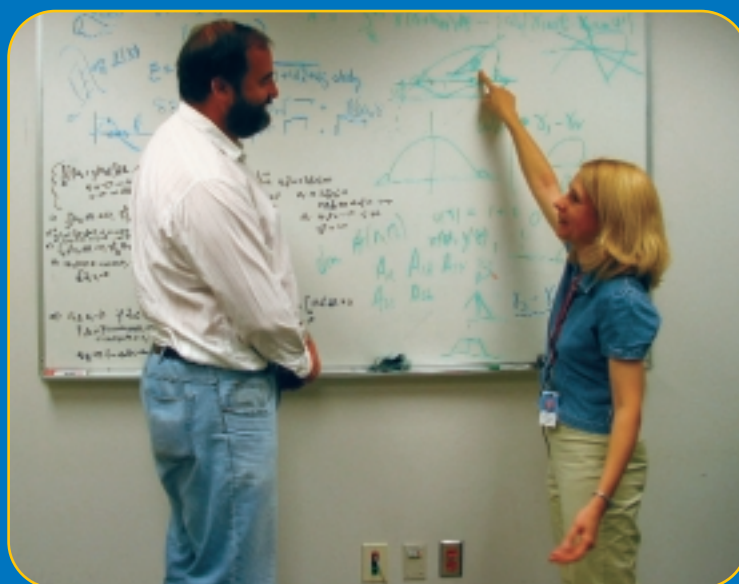
ITL's development, measurement, and standardization of general-purpose mathematical software tools, along with related information services, contribute to an improved environment for computational science research within NIST and in the scientific community at large. Work areas include interfaces and software for numerical linear algebra, algorithms and software for parallel adaptive multigrid solution of partial differential equations, and Java™-based technologies for numerical computing. Our work is carried out in collaboration with industry consortia and working groups, national laboratories, and academia.

In FY 2002 we published a standard for Sparse Basic Linear Algebra Subroutines (BLAS) in collaboration with the BLAS Technical Forum. We developed an ANSI C BLAS reference implementation and completed the accompanying test suites. We released Parallel Adaptive Multigrid Methods and Software (PHAML) Version 0.9, a parallel adaptive partial differential equation solver written in Fortran 90 using MPI. We incorporated related NIST algorithms and software into the Zoltan Library of Sandia National Laboratories for dynamically load-balancing

parallel applications. We released Version 1.01 of the Template Numerical Toolkit (TNT), an object-oriented library of standard linear algebra operations based on C++ templates.

We continue to operate popular web-based information services. The Guide to Available Mathematical Software (GAMS), our cross-index and virtual repository of general-purpose mathematical software components, provides access to some 9,000 items from more than 100 packages. The Matrix Market is a database of matrices used in studies of algorithms and software for linear algebra. Our Java™ Numerics website provides information on numerical computing in Java, including a standardized web-based benchmark, called SciMark. The current high score for SciMark is over 300 Mflops, a 44 percent improvement over one year ago. These services are among the most popular at NIST.

As a result of this work, NIST scientists and engineers, as well as the larger computational science community, benefit from more accurate, reliable, portable computational modeling, greater ease in developing technical computing applications, and improved portability and performance of technical computing applications. The website is <http://math.nist.gov/>.



Geoffrey McFadden and NRC Research Associate Katharine Gurski apply mathematical methods to a variety of problems, from the formation of dendritic crystals to the stability of quantum wires.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

STATISTICS



Alisha Sparks, a student in the Statistical Engineering Division, and Ken Butcher, NIST Technology Services, discuss the statistical analysis of U. S. and proposed European standards for packaging and labeling.

Comparison; the implementation, testing, and comparison of several Bayesian partition models; and a general purpose MATLAB implementation of the normal Bayesian hierarchical model.

Elicitation of prior information and quantification of expert opinion is key to using Bayesian methods to their full capacity. We are adapting available methodology and developing specialized software to assist the NIST scientific community in this endeavor. For linear models we have completed a prior elicitation of hyperparameters using conjugate priors based on a quantile elicitation approach. In a parallel effort we also completed a prior elicitation for hyperparameters in multivariate linear models drawing on historical data. Graphical representations of Bayesian inferences and diagnostics are being developed, implemented, and prepared as web-based products. The website is <http://www.itl.nist.gov/div898/bayesian/homepage.htm>.

BAYESIAN METROLOGY

Scientists at NIST and national metrology laboratories routinely use Bayesian methods for standard uncertainty analysis. Bayesian statistics provide a unified framework for optimally combining information from multiple sources, resulting in highly efficient experimental designs and statistical analyses. We continue to expand fundamental statistical theory necessary for the application of statistics to metrology; at the same time we are developing and implementing specialized Bayesian methods to metrology research at NIST and in the international metrology community. In FY 2002, we presented nine talks at national and international conferences, published eight papers, and taught courses on Bayesian statistical and linear models. Methodology development included both software implementation for Bayesian metrology and the developing of standard reference data sets for the evaluation of Markov Chain Monte Carlo algorithms. Successful application of Bayesian statistics for metrology has spanned the analysis of an international Key

KEY COMPARISONS AND UNCERTAINTY

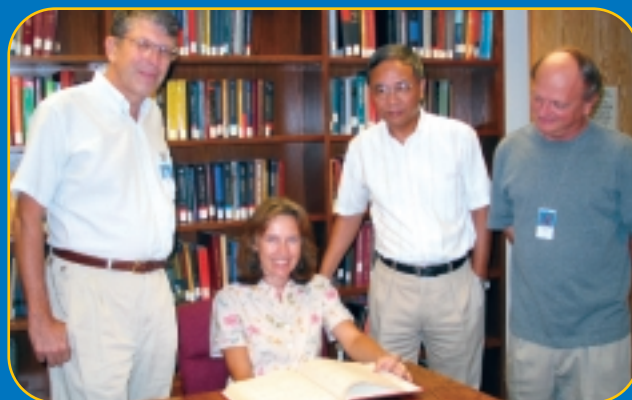
International Key Comparisons serve as the technical basis for acceptance of measurements by member laboratories participating in the Mutual Recognition Agreement (MRA) of the National Metrology Institutes (NMIs) worldwide. ITL leads a collaborative effort with other NIST laboratories and NMIs to ensure that sources of statistical variation are correctly identified. This includes determining whether two national laboratories have comparable measurements and assessing the differences among participating laboratories using statistical methods. In FY 2002, we collaborated with scientists in NIST's Chemical Science and Technology, Electronics and Electrical Engineering, Manufacturing Engineering, and Physics Laboratories by collecting and analyzing data for seven Key Comparisons in which NIST participated. New work in statistical design led to a set of candidate designs for collection of data in six upcoming Key Comparisons on fluid flow. Statistical Engineering staff presented an invited tutorial on design principles and specific options to the international Working Group on Fluid Flow.

In addition to participating in individual Key Comparisons, we initiated a focused statistical research effort on the foundations of key comparisons in order to provide general guidance and computer tools for the design and analysis of key comparisons. We formulated an approach to the performance evaluation of commonly applied parametric, nonparametric and Bayesian methodologies for estimating the key comparison reference value (KCRV) and the associated uncertainty. Specific Key Comparisons have required new statistical research. We have applied the new methodology, presented it to the scientific community, and published results, for example, the uncertainty analysis for Key Comparisons when traveling standards are subject to drift effects over time.

Statistical Engineering Division staff took an active international role, participating in meetings held under the auspices of several Consultative Committees of the International Committee for Weights and Measures (CIPM) and the Joint Bureau International des Poids et Mesures/ National Physical Laboratory (BIPM-NPL) Workshop on the Impact of Information Technology in Metrology, with a formal presentation at the satellite workshop on Evaluation of Interlaboratory Comparison Data. We continue a major research effort to provide the scientific metrology community with more accurate uncertainty assessment and computation methodology to improve scientific decision-making. The website is <http://www.itl.nist.gov/div898/projects/keycomp.htm>.

STATISTICAL ANALYSIS OF IT PERFORMANCE

ITL is defining the measures of IT performance and determining their statistical characteristics. To accomplish this, we construct models to assess the importance of factors in performance of networks and biometrics, provide a statistical basis for IT standards, and construct efficient experimental designs for IT applications for computer forensics, speech recognition, and document understanding. In FY 2002, we collaborated with ITL's Advanced Network Division to develop sound statistical methodology for network traffic data analysis and simulation, with potential applications for Quality of Service (QoS) and computer security. For the HumanID project, we focused on solutions to the algorithmic comparison problem in face recognition. In computer forensics, we provided a statistical-based rigorous foundation for the



Andrew Rukhin, Blaza Toman, Nien-Fan Zhang, and Stefan Leigh discuss statistical approaches to uncertainty analysis for International ("Key") Comparisons Among National Metrology Institutes.

National Software Reference Library and the Computer Forensics Tool Testing projects. We contributed to speech recognition research by translating the problem into appropriate statistical essentials and prioritizing the experimental design and analysis. Lastly, we consulted on ITL's document understanding project. The website is <http://www.itl.nist.gov/div898/itperf/homepage.htm>.

STATISTICAL COLLABORATIONS AND MEASUREMENT SERVICES

ITL collaborates with the NIST staff on research projects where optimal experiment design, statistical modeling, and data analysis play a significant role in improving measurement processes and gaining scientific insight. We design and analyze experiments and evaluate uncertainties for the NIST Standard Reference Materials (SRMs) and Calibration Programs. In FY 2002, we maintained and supported NIST's role as the highest quality SRM service in the United States, contributing to the development and certification of more than 40 SRMs. We developed an administrative database to track individual SRMs, which allows for more effective monitoring and reporting.

As part of the Statistical Engineering Division's interdisciplinary collaborative role in NIST science, extensive long-term collaborations continue to break new scientific ground in the areas of subatomic particle lifetime, optoelectronics, and low-level radionuclide measurement. Other collaborations that contribute directly to



*The e-Handbook of Engineering Statistics Development Team:
Thomas Ryan (consultant), Alan Heckert, Carroll Croarkin,
James Filliben, and Will Guthrie.*

American industry and to American consumers include cigarette flammability, highway concrete lifetime and cost optimization, optical particle counters, and gas metrology calibration. The websites are <http://www.itl.nist.gov/div898/consult/consult.html> and <http://www.itl.nist.gov/div898/projects/srm.htm>.

STATISTICAL METROLOGY EDUCATION

ITL offers statistical short courses and tutorials, which are tailored to NIST science and metrology. Topic areas include statistics, probability, data analysis, and statistical computing. These core courses in statistical concepts and methodology are supplemented by special topics on an as-needed basis. The training provides researchers with the statistical tools necessary to improve the quality of experimental design and analysis at NIST. We also offer hands-on work experience for students and interns in statistics; seven undergraduate and graduate students spent the summer of 2002 working on statistical metrology in the Statistical Engineering Division.

In July 2002, the NIST/SEMATECH e-Handbook of Engineering Statistics was officially released. Within a month, the e-Handbook became the top citation for web searches on "engineering statistics." The e-Handbook began when ITL teamed up with International SEMATECH, a consortium of worldwide major semiconductor companies, to provide this

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. The final editing, incorporating new features suggested by beta-test users, is also available as the e-Handbook CD. The website is <http://www.itl.nist.gov/div898/handbook/index.htm>.

STATISTICAL PROCESS CHARACTERIZATION

ITL statisticians work with NIST scientists and with industrial partners to characterize complex processes and to address measurement and standards aspects of physical science, engineering, and IT. For NIST's Electronics and Electrical Engineering Laboratory, we collaborated in the dielectric materials metrology work by completing an uncertainty analysis and developing code for software for computing permittivity and loss tangent; the software was made available to industry in August 2002. Consulting in high-speed optoelectronics, we developed a method for estimating the bias of timebase distortion estimates and released public domain software for correction of signals for drift, jitter, and timebase distortion. In collaboration with NIST's Chemical Science and Technology Laboratory, we developed a full-blown example of the sequential approach to designing a series of experiments to characterize a new measurement process and to identify all the critical factors. This example was based on the dual meter flow measurement system comparison characterized at NIST and now to be used in fluid flow calibrations in both national and international arenas. For the U.S. electronics and communications industries, we developed accurate calibration and measurement techniques for nonlinear network analysis. Also for industry, we contributed to a quantitative measurement system for neutron depth profiling. The website is <http://www.itl.nist.gov/div898/charact/homepage.htm>.

SELECTED CROSS CUTTING THEMES

BIOMETRICS

ITL is developing interoperable open standards, guidelines, and specifications for biometric systems. Our experience includes standards development, design of experiments, statistical analysis, algorithm development, distributed computing, image processing, software engineering, systems integration, and signal processing.

In collaboration with the NIST Building and Fire Research Laboratory, ITL is developing test methodologies, documentary standards, and reference implementations (software and hardware prototypes) to assist the biometrics industry and end-users in the testing and deployment of scalable, integrated biometric systems. The impact of this research will: a) lower the technical engineering investments needed for developing and modifying state-of-the-art biometric systems, b) enable the integration of biometric systems with building automation systems, and c) clarify subsystem and middleware requirements to get more biometric-compatible installation points in buildings. Biometric technologies have been used for single point solutions; e.g., entry access, computer log-on. This project seeks to explore the scalability of biometrics systems for large enterprise environments, and the subsequent development performance metrics and test methodologies. In FY 2002, we began development of an open, performance evaluation laboratory to examine different biometric systems. Work progressed on the software development of a Linux version of the BioAPI standard, which became an ANSI standard. We continued our leadership in the Biometrics Consortium and held two major conferences this year featuring biometrics and its application as a homeland security technology. More than 900 persons and over 70 exhibitors participated in our September 2002 conference.

For the Department of Justice, the FBI, the National Institute of Justice, developers, vendors, and law enforcement organizations, we are providing standards and evaluation technology for interoperable Criminal Justice Information Systems (CJIS). We published NIST Special Databases 29 and 30 for plain and rolled images from paired fingerprint cards. We completed the NIST Fingerprint Image Software (NFIS) package and distributed 333 copies of the CD. We also published the revised



Fernando Podio, Mike Indovina, Alan Mink, Barry Hershman, and Robert Snelick test the performance of an iris scan device in the NIST biometrics system integration and engineering laboratory.

XML Rap Sheet Transmission Specification and initiated the development of the Verification Test Bed (VTB). ITL fulfills its mandate to certify biometrics under the USA Patriot Act by determining estimates of performance for fingerprint and face biometrics using several NIST special databases. Using large operational fingerprint and facial databases from federal agencies, we developed an initial NIST VTB for testing fingerprint verification scores. To fill the need for accurate biometrics for border security as part of homeland defense, we ran verification tests on Immigration and Naturalization Service (INS) databases.

Funded by the Defense Advanced Research Projects Agency and the National Institute of Justice, ITL's Human Identification at a Distance (Human ID) project focuses on providing evaluation methods and test data for biometric systems that operate at long distances from the subject. Since September 11, 2001, our work has focused on certifying the accuracy of face verification of individuals using visas and on border security. In FY 2002, we designed and gathered imagery for a large-scale Face Recognition Verification Test. We implemented a baseline gait recognition system and distributed it to the research community. The ITL Biometrics Resource Center website is <http://www.nist.gov/biometrics>.

SELECTED CROSS CUTTING THEMES

CRITICAL INFRASTRUCTURE PROTECTION



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

Protecting the nation's vital infrastructure has become a top priority since the tragedy of September 11, 2001. U.S. government operations, business and commerce, and the health and safety of the American public rely upon a national information infrastructure and supporting physical infrastructure, such as telecommunications, energy, financial services, water, and transportation sectors. Many of the systems and physical assets of these infrastructures are critical to the nation's security, economy, or health and safety. Information technology (IT) advances have caused these infrastructures to become increasingly automated and interlinked, creating new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks.

Consistent with its overall mission and long-standing security responsibilities in information technology, ITL focuses on security standards and testing to help ensure the security of our nation's critical infrastructures. We support federal departments and agencies under the Computer Security Act of 1987 and follow-on legislation that assign to NIST responsibility to develop security standards and guidelines for sensitive 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 infrastructures.

SELECTED CROSS CUTTING THEMES

PERVASIVE COMPUTING

ITL's pervasive computing initiative is a natural fit for our organization. The initiative builds upon our robust R&D programs in human computer interaction, such as speech and visual recognition and tracking, sophisticated information access from multimedia databases, extensive information presentation capabilities, dynamic networking, wireless networking, software testing, and security.

A significant component of our pervasive computing effort is our smart space testbed. We advance smart space technologies and accelerate their deployment by providing a modular testbed for integration, interoperability, architecture development, data collection, and performing experiments. In FY 2002, we deployed our Smart Flow System to our Meeting Room, which includes hundreds of sensors and terabytes of data. We integrated wireless capability for using personal digital assistants (PDAs). We produced a new microphone array with onboard analog to digital conversion. We are also developing a usability-enhanced Smart Flow System, which is much easier to install and program. We serve on the founding editorial board of the IEEE Pervasive Computing Magazine. Our Pervasive Computing 2002 Conference was held in early October 2002, with an emphasis on medical pervasive computing applications. The website is <http://www.nist.gov/smartspace>.

The software system components of our pervasive computing initiative focus on applying Architecture Description Languages (ADLs) to Service Discovery Protocol (SDP) specifications and our Aroma project, which is developing measurements and tools for pervasive computing. This year we modeled Universal Plug and Play (UpnP) and developed two-party and three-party Rapide architectural models to cover all SDPs. We produced metrics for industry analysis of distributed component systems in harsh conditions, analyzed SDPs, and published four reports on the work. We continued the development and use of our Existential Simulation

Tool (EXiST); our redesign of the tool around XML-based web services allows for portability, interoperability, and extensibility. We also created a database for measurements. The website is <http://www.itl.nist.gov/div897>.



College students Stephanie Gantt, Peng Ying, and Alexandria Chambers learn about pervasive computing tools and techniques as part of their projects in ITL.

We continued to address networking issues for pervasive computing. To expedite the development of wireless personal area networks (WPANs), we worked with IEEE 802.15 to complete one specification, developed specification and description languages (SDLs) for two specifications and one protocol implementation conformance statement (PICS), produced a recommended practices document on coexistence, and published ten papers on interference and coexistence. We also developed a generic model for service discovery (SD) protocols, studied and published three papers on resiliency of SD protocols, and shared the results with Sun Microsystems, Inc., and the UPnP forum. Our work is helping the IT industry to understand the technical properties of various industry dynamic discovery and configuration technologies. The website is <http://w3.antd.nist.gov>.

SELECTED CROSS CUTTING THEMES

QUANTUM INFORMATION



Richang Lu, Xiao Tang, Mikko Heikkero (seated), and Alan Mink designed and engineered the optics and electronics for the NIST Quantum Communications Testbed.

NIST's quantum information program was initiated in response to the coming confluence of computer science and quantum physics. The goal of the program is to understand the implications of the use of quantum states of matter to represent, process, and communicate information and to begin to develop the new IT infrastructure necessary to support it. Quantum information could provide benefits in many areas. Perfectly secure communications and the ability to solve problems beyond the capabilities of classical computers in applications such as code breaking and pattern matching could have a profound impact on homeland security. For commerce and trade, advances in quantum information could lead to more secure electronic commerce and continued maintenance of the U.S. lead in the computer technology marketplace.

ITL contributes to NIST's interdisciplinary quantum information program (in collaboration with the Physics and Electronics and Electrical Engineering Laboratories) in the areas of applied mathematics, algorithms, computing and communications architecture, computer security, and network protocols; five ITL divisions contribute to the program. ITL's work is in two broad arenas: quantum

communication and quantum computation. We are developing a quantum communication testbed facility for technology assessment and integration, showcasing hardware and protocols for cryptographic key distribution based on commercially feasible technologies, with the attainment of Mbps effective transfer rates as the goal. In FY 2002, we completed the design of a 600 meter free-space 1.25 GHz optical wireless link containing both quantum and classical channels. Laboratories at each end of the link were renovated, and necessary equipment, such as telescopes and high-speed electronics, was procured. We designed data collection hardware, implemented a cryptographic key exchange software system, implemented and tested the application programming interface (API), and began the testbed assembly. In addition, to improve the reliability of identity verification for network applications, we devised and documented a hybrid quantum authentication scheme and filed a provisional patent application.

In the area of quantum computation, we are working on fundamental problems at all scales, from the modeling of physical realizations of quantum bits (qubits), to architectural concepts for quantum computers, to the development of quantum algorithms. In FY 2002, we developed mathematical methods to compute trapping states for neutral atoms in optical lattices from the Schrödinger equation model, extending ITL's parallel adaptive partial differential equations solver PHAML to use them. We developed the concept of a quantum bus architecture based on entanglement swapping and teleportation, and began analysis of its scalability and error properties. We developed software to enumerate quantum circuits (i.e., fundamental algorithmic components) for Boolean functions. Finally, we developed a novel algorithm to determine whether a finite integer function is one-to-one.

As we build expertise in the uses of quantum computing and communication, ITL's world class IT program can significantly advance the development of the next generation of information technology. The web page is <http://math.nist.gov/quantum/>.

ACCOMPLISHMENTS OF OUR SERVICES PROGRAM

BUSINESS APPLICATIONS

ITL provides centralized, comprehensive support for a variety of business applications and administrative systems at NIST. In FY 2002, we provided system administration for the new Grants Management Information System. For the NIST e-Approval system, we completed the rollout and training for 62 percent of the 3,200 targeted users; more than 10,000 actions were processed through e-Approval in FY 2002. We supported the development of the e-Approval-based NIST Associate Information System. For the NIST KnowledgeNet, we implemented user-requested enhancements, a help module, and an external reporting capability. Our support for the Commerce Administrative Management System (CAMS) continued, with a FY 2003 deployment date. By supporting these critical services, ITL ensures a secure and efficient business environment throughout the agency. The website is <http://www.itl.nist.gov/div896/>.

CHIEF INFORMATION OFFICER (CIO)

The Office of the NIST CIO resides within ITL. The CIO provides centralized business-level planning and program management for all NIST information technology (IT) resources and programs. The office administers the NIST IT Strategic Plan, the NIST IT Operations Plan, the NIST Systems Development Life Cycle, the NIST IT Architecture Plan, and NIST's implementation of the government-wide 508 Accessibility program. In FY 2002, we initiated the Security Access Control Project and issued NIST policies on Persistent Cookies. We represented NIST at Department of Commerce (DoC)-sponsored groups and oversaw the actions of the NIST Information Technology Services Planning Team (ITSPT). We also implemented the IT Capital Asset Planning for Supercomputing funds and initiated a consolidated NIST IT services contract. We planned for the implementation, in FY 2003, of an entirely new CIO organization.



The PC Buying Service Team offers a convenient way to purchase a computer that meets the Information Technology Services Planning Team's (ITSPT) requirements for implementation of a NIST-wide uniform desktop system. Team members include Ricky Hilderbrand, Jason Barnard, Eric Konig (leader), Paul DeBruin, Denise Miller, and Dan Diamond.

DESKTOP COMPUTING

ITL's managed desktop program includes over 1,000 desktops to date. Our asset management program advanced in FY 2002 with the development of a web-based IT Asset system, which was integrated with the LANDesk automated inventory capabilities. We launched a PC Buying Service so NIST staff can purchase a computer that meets ITSPT requirements for implementation of a NIST-wide uniform desktop system. Over 70 percent of NIST PCs purchased during the year were bought through the buying service, a total of more than 800 computers. We upgraded the desktop model to a Pentium IV and added laptop and high-end workstation models. The website is http://www.itl.nist.gov/itl_serv.html.

ENTERPRISE SERVERS

ITL operates the central NIST servers, such as e-mail, calendar, and application servers. In FY 2002, we implemented disaster recovery procedures and capabilities for all major systems. We completed a full disaster recovery test for administrative processing and completed local disaster recovery tests for other systems. We implemented a new high availability central e-mail server. For web services, we moved to a high availability environment for internal web services and implemented a web application development environment. The website is <http://www.itl.nist.gov/div896>.



*The original iTAC team:
Tom Lacko, Linda Helfer
(Team Leader), Laura Hanlon,
Carolyn Holmes, Angela Beattie,
Charlette Prather, Stephanie
Auchmoody, and Omar Andrade.*

ITAC CENTRAL HELP DESK

To provide improved IT support and response time to our NIST customers, ITL launched its iTAC Central Help Desk in Gaithersburg and Boulder. Since its inception, ITAC has averaged over 1,500 requests per month. We developed a monthly service metrics report and implemented multi-mode outage notification processes.

INFORMATION TECHNOLOGY SECURITY OFFICE (ITSO)

ITSO provides NIST with a central resource for addressing security issues, providing security training to the NIST staff, responding to incidents, and issuing security policy, procedures, and guidance. In FY 2002, ITSO developed and issued a Password Management Policy and acquired 100 percent user compliance certification; directed the deployment of the e-NIST DMZ Firewall to protect over 75 NIST public servers on three networks and the NIST modem pool; sponsored several specialized security training sessions and provided IT security training to 100 percent of the NIST staff; managed the first annual NIST IT Security Day at Gaithersburg and Boulder, attended by over 2,000 NIST staff; developed draft policies on certification and accreditation, and patch management, and updated the NIST IT Security Program Policy; developed and issued

guidance on several security issues including system hardening, risk assessments, contingency planning, and certification and accreditation; developed and directed the certification and accreditation program, completing certification and accreditation of 100 percent of NIST's systems; responded, directed, and assisted with the response and cleanup of virus-related and hacker incidents; directed the completion of FY 2002 Government Information Security Reform Act requirements, including self assessments of 100 percent of NIST's systems; participated in technical security reviews of several new NIST applications and systems, such as e-Approval, Grant Management Information System, Commerce Administrative Management System, Data Warehouse, etc.; and participated in the Office of Inspector General (OIG) Government Information Security Reform Act evaluation of NIST and the OIG audit of NIST financial systems. The ITSO website is located at <http://www.nist.gov/its>.

NETWORKING

ITL provides a wide range of networking services to the NIST staff. In FY 2002, we upgraded webcasting performance and encoding capabilities at NIST, while webcasting two or three events per week. We completed the migration of three buildings to universal wiring. We implemented a fiber infrastructure for most buildings to support the Gigabit backbone network. We implemented the network infrastructure for the e-NIST firewall and public network. We maintained a 99.8 percent availability of NISTnet. Our telecommunications staff continued to provide reliable service to NIST users, while implementing a prototype teleworker capability. Security audits were also performed in Gaithersburg and Boulder. The website is <http://www.itl.nist.gov/div896>.

SCIENTIFIC COMPUTING

NIST scientists and engineers require complex, sophisticated high-performance scientific computing capabilities. ITL provides standardized scientific computing architectures that allow ready access to and networking of high-end workstations, parallel computing clusters, and supercomputing facilities (both internal and external to NIST) and enable maximum use of collective memory and processing capacities, as necessary, for the conduct of NIST research. In FY 2002, we retired an SP2 cluster. We completed an initial test of the Globus Grid computing environment. In our PC Cluster, we upgraded from 64 to 128 CPUs. Lastly, we coordinated a survey of user requirements for scientific computing at NIST. The website is <http://www.itl.nist.gov/div896>.

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. In addition to three Cooperative Research and Development Agreements (CRADAs) with industry in FY2002, we participated in many consortia and industry interest groups, including the following:

ADVANCED TELEVISION SYSTEMS COMMITTEE (ATSC)

The ATSC establishes voluntary technical standards for advanced television systems. ITL staff members Alan Mink, Robert Snelick, and Wayne Salamon participate in T3/S17, Digital TV Applications Software Environment (DASE) Application Programming Interface (API). ITL has been a catalyst for the approval of an interactive digital television standard.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

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



Lattice Boltzman simulation of the Taylor-Tomotika instability of a fluid thread confined within a tube.

ASTM

ASTM (American Society for Testing and Materials) is a not-for-profit 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.

BASIC LINEAR ALGEBRA SUBPROGRAMS (BLAS) TECHNICAL FORUM

The BLAS Technical Forum is an industry/government/academic working group, which is developing community standards for sparse matrix operations and extending the BLAS to new domains. Roldan Pozo chairs the sparse matrix subcommittee. Through participation in the forum, ITL contributes to the development of interface specifications and reference implementations for BLAS.

BIOMETRIC APPLICATION PROGRAMMING INTERFACE (BIOAPI) CONSORTIUM

The BioAPI Consortium is an organization of over 100 members including IT organizations, biometric vendors, and users. It is international in nature (30 percent of the members are from overseas). The Consortium developed the BioAPI specification. It became an ANSI-INCITS

standard (InterNational Committee for Information Technology Standards) in February of 2002 through the INCITS fast track process: ANSI/INCITS 358, the BioAPI specification v1.1. Fernando Podio is a member of the BioAPI Steering Committee and chairs the BioAPI External Liaisons Task Group, which was responsible for transitioning the specification to formal standards bodies.

BIOMETRIC CONSORTIUM (BC)

The Biometric Consortium serves as the U.S. 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 NIST/Biometric Interoperability, Performance and Assurance Working Group and the Common Biometric Exchange File Format Group. ITL was instrumental in the development of this standard.

COMMON CRITERIA MANAGEMENT COMMITTEE

This group of 14 industrialized nations formed a cooperative agreement to recognize the results of security testing of IT products and systems conducted by accredited, independent, third party testing laboratories. Stuart Katzke chairs the Common Criteria Management Committee Executive Subcommittee. ITL's leadership in this area benefits government and industry by increasing the availability of commercially tested IT products necessary to build more secure systems and networks for critical infrastructure applications.

CROSS INDUSTRY WORKING TEAM (XIWT)

The XIWT is a multi-industry coalition of information technology 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.



ITL is developing interoperable open standards, guidelines, and specifications for biometric systems.

DVD ASSOCIATION (DVDA)

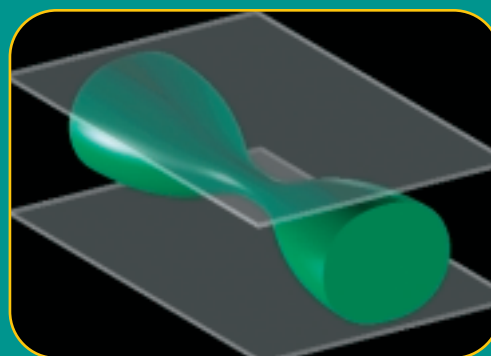
The DVD Association represents standards developers, software developers, disc and electronics manufacturers, government agencies, and content developers for DVD technology and associated technologies. Victor McCrary represents ITL. Through our representation, we are facilitating standards, interoperability, and compatibility for writable DVD media, disc drives, and consumer electronic players.

FINANCIAL SERVICES TECHNOLOGY CONSORTIUM (FSTC) FAST WORKING GROUP

ITL participates with FSTC in its FAST (Financial Agent Secure Transaction) project. FAST addresses e-commerce participants with concerns about valid identities for other web parties, characteristics being claimed, promised or contracted for (examples are payment guarantee, shipping reliability or rights of product use, and privacy for personal data and business marketing information. Gordon Lyon represents ITL. Our support promotes economical trust and assurance for e-commerce.

FORUM ON PRIVACY AND SECURITY IN HEALTHCARE

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 forum 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.



Lattice Boltzmann simulation of breakup of a fluid thread confined between parallel plates.

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 and John Barkley represent ITL in the HL7 Conformance Special Interest Group.

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 that makes it possible for the industry to improve the interoperability and performance of their products for the increased demands for high-density data storage.



Jack Wang, Hari Iyer, Duane Boes, and Jolene Splett discuss issues in the ISO Guide to the Expression of Uncertainty in Measurement.

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. Daniel Benigni serves on the Board of Governors of the IEEE Standards Association. Sharon Laskowski participates in P2001, Web Best Practices Working Group. David Cypher, Robert Van Dyck, Nada Golmie, and Nader Moayeri participate in IEEE 802.15, Working Group for Wireless Personal Area Networks, and Nader Moayeri also attends IEEE 802.16, Working Group on Broadband Wireless Access Standards. Finally, Larry Reeker 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 Policy and Procedures Committee. ITL technical staff participate in many working groups, including biometrics (chaired by Fernando Podio), coding of audio, picture, multimedia and hypermedia information (chaired by Mike Rubinfeld), data representation, IT access interfaces, IT security techniques, MPEG development, open distributed processing, and still image coding. Through these interactions, we contribute our expertise to the development of IT industry standards.

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.

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP)

ITL's Ronald Boisvert chairs the IFIP Working Group on Numerical Software (WG2.5), which is part of the IFIP Technical Committee on Programming Languages (TC 2). WG2.5 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, Doug Montgomery, and Nader Moayeri participate in the Routing Area; Okhee Kim, Doug Montgomery, Sheila Frankel, Nelson Hastings, and Tim Polk participate in the Security Area; and Doug Montgomery and Mudumbai Ranganathan participate in the Transport Area.

JAVA™ GRANDE FORUM

The Java™ Grande Forum (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 has worked with Sun Microsystems to implement changes in Java's specifications which admit much faster execution (up to ten times faster) for computing-intensive applications.

JTC1 TAG

The Joint Technical Committee 1 (JTC1) develops, maintains, promotes, and facilitates IT standards required by global markets meeting business and user requirements concerning the design and development of IT systems and tools. Michael Hogan represents ITL on the U.S. TAG to ISO/IEC JTC1 on Information Technology, ensuring that ITL has a voice in global IT standards development.

MICROMAGNETIC MODELING ACTIVITY GROUP (MUMAG)

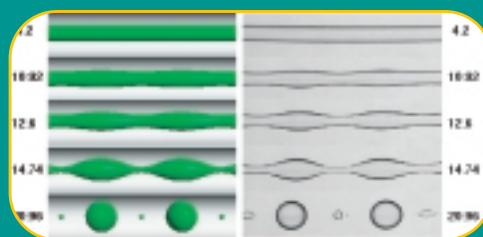
muMAG is an organization of industrial, government, and academic researchers investigating fundamental issues in micromagnetic modeling through the establishment of standard problems for testing micromagnetic simulation software and the development of a public domain reference implementation of micromagnetic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

NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)

NIAP is a NIST/NSA partnership for testing methods and measures to ensure the quality of information security systems. ITL's Ronald Ross serves as Director of NIAP. Our involvement helps to ensure that the security testing needs of federal and industry IT consumers and producers are met.

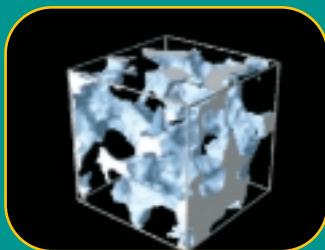
NORTH AMERICAN OPEN MATH INITIATIVE (NAOMI)

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



Comparison of experimental data with a lattice Boltzmann simulation of fluid thread breakup.

Portion of a sandstone sample used in the simulation of fluid flow through porous media.



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. ITL's participation includes the development of conformance tests for these standards.

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.

OPEN GROUP

The OPEN GROUP focuses on the development and implementation of a secure and reliable IT infrastructure. Shu-Jen Chang participates in Security Services.

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)

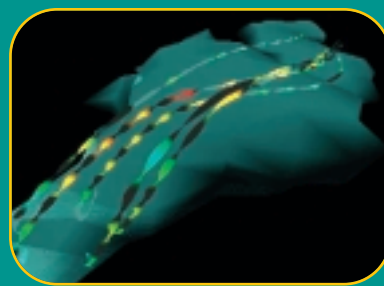
OSTA is an international trade association dedicated to promoting the use of writable optical technology for storing computer data and images. Xiao Tang represents ITL.

ROSETTANET EBUSINESS STANDARDS CONSORTIUM

RosettaNet is an independent, self-funded, nonprofit consortium dedicated to the development and deployment of standard electronic commerce interfaces to align the processes between IT supply chain partners on a global basis. Thomas Rhodes represents ITL.

SMART CARD SECURITY USERS GROUP (SCSUG)

SCSUG develops and promotes the use of standardized security requirements to ensure that the device security and data protection needs of the smart card end users are appropriately represented and met in smart card products. SCSUG is composed of the major worldwide credit card brands (financial payment systems): American Express®, Europay, JCB, MasterCard®, Mondex™, and Visa®. Stuart Katzke represents ITL.



The figure shows a visualization of a cloud water dataset derived from a sample dataset and program provided by the Open Visualization Data Explorer (OpenDX) software package.

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. Randall Easter participates in the Study Group on Conditional Access for Digital Cinema. Charles Fenimore represents ITL on the Video Quality Experts Group.

VIDEO ELECTRONICS STANDARDS ASSOCIATION (VESA)

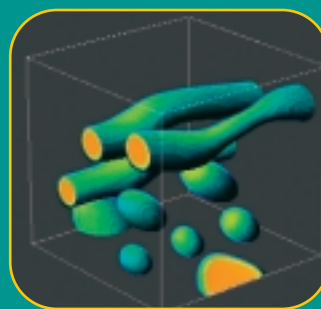
VESA promotes and develops timely, relevant, open display and display interface standards, ensuring interoperability and encouraging innovation and market growth. John Roberts represents ITL on four committees in this organization. As a member of VESA, ITL participates in the technical development of standards and develops laboratory implementations of proposed interface architectures.

WEB3D CONSORTIUM

The Web3D Consortium provides an open 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.

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 Advisory Committee. ITL staff members serve on a host of committees within this organization, including the Quality Assurance Activity, the Cascading Stylesheets (CSS) Working Group (WG), the Document Object Model (DOM) WG, the Extensible Markup Language (XML) Protocol WG, the Extensible Stylesheet Language



Simulation of phase separation of a mixture of two fluids under shear.

(XSL) WG, the Math WG, the Schema WG, the SYMM WG, and the XML Working Group. 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 Committee, 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. ITL promotes the security of the financial services industry through participation in this forum.

STAFF RECOGNITION



(from left) Donald L. Evans, Secretary of Commerce, Rick Kuhn, John Barkley, Dave Ferraiolo, Benjamin Wu, Deputy Under Secretary, Technology Administration, and Arden Bement, NIST Director

DEPARTMENT OF COMMERCE 2002 MEDAL AND NIST AWARDS

John Barkley, Software Diagnostics and Conformance Testing Division, and **David Ferraiolo and Richard Kuhn**, both of the Computer Security Division, received the Department of Commerce Gold Medal for scientific/engineering achievement in creating, developing, and transferring the Role-Based Access Control (RBAC) technology to private industry.

Michael Donahue and Donald Porter, Mathematical and Computational Sciences Division, received, with NIST colleague Robert McMichael, the Bronze Medal Award for scientific and engineering achievement in the advancement of computational techniques for simulating the behavior of micromagnetic materials.



Walter Liggett, Jr., Statistical Engineering Division, along with NIST colleagues **Samuel Low and Jun-Feng Song**, received the 2002 Judson C. French Award for developing a framework for providing traceability to U.S. national standards in the area of Rockwell C-scale hardness testing.



William Majurski, Software Diagnostics and Conformance Testing Division, received the Bronze Medal Award for scientific achievement in the design and development of distributed models, architectures, and reference implementations of healthcare information systems.

EXTERNAL RECOGNITION

William Burr, David Cooper, and Tim Polk, Computer Security Division, were recognized at a ceremony at the White House Conference Center at the inauguration of the Federal Bridge Certification Authority (FBCA). Burr was recognized as a "Founding Father" of the FBCA. Cooper and Polk were cited for their unparalleled contribution to the development and operation of the FBCA, which provides a new secured way for federal

agencies to exchange information, with each other and with their constituents.



Wo Chang, Information Access Division, received recognition from the World Wide Web Consortium (W3C)'s Synchronized Multimedia (SYMM) Working Group (WG) for his contribution of hosting and editing the Synchronized Multimedia Integrated Language (SMIL) 2.0 interoperability test suite. W3C viewed the interoperability test suite as vital for SMIL 2.0 to become a W3C Recommendation. The SMIL 2.0 Recommendation represents a cross-industry agreement on an XML-based language that allows authors to write interactive multimedia presentations.



The Network Journal honored **Alicia Clay**, Computer Security Division, in their annual 40-Under-Forty Achievement Awards program. The awards recognize individuals across industry lines that have achieved significant levels of success and made substantial contributions in their areas of business and community service. Clay organizes regional workshops for small businesses across the nation.



Dianne O'Leary (left) and **David Gilsinn**, Mathematical and Computational Sciences Division, together with NIST colleague **Geraldine Cheok** (right), won the Best Paper Award for their contribution to the 19th Annual Symposium on Automation and Robotics



in Construction (ISARC 2002). Their paper, entitled "Reconstructing Images of Bar Codes for Construction Site Object Recognition," was selected as top paper of the 88 manuscripts from 20 countries that were accepted for presentation. Their paper describes techniques for the automated recognition of bar codes from LADAR (laser distance and ranging) optics.



Michael Hogan, ITL Office of the Director, received the National Committee for Information Technology Standards (NCITS) 2001 Chairman's Annual Award. Hogan was honored for "his dedication to NCITS and success in expanding its program of work. His long-term commitment to procedures,

institutional memory and the 'good of the organization' serve as a strong foundation for the vision and opportunities he brings to NCITS."



Kevin Mills (center), Advanced Network Technologies Division, led an ITL research team that received the 2001 Bytes for the Buck award, given annually to DARPA's Active Networks project judged most productive and cost-effective. In addition to Mills, the team included **Stefan Leigh** (left) and **Andrew Rukhin** (right), Statistical Engineering Division, and Virginie Galtier and Yannick Carlinet, guest scientists from Loria Université Nancy and Ecole des Mines Nancy, respectively. The ITL team focused on developing a standard means to specify processor (CPU) demands for mobile computer programs, also known as mobile code.



Victor McCrary, Chief, Convergent Information Systems Division, received the prestigious Percy Julian Award from the National Organization for the Professional Advancement of Black Chemists and Chemical Engineers (NOBCCHE). This is the highest award given by NOBCCHE for significant achievement in pure and applied research.



Geoffrey McFadden, Mathematical and Computational Sciences Division, was elected a Fellow of the American Physical Society (APS). McFadden was recognized "for fundamental insights into the effect of fluid flow on crystal growth and for an innovative approach to phase field methods in fluid mechanics."

McFadden has published more than 100 papers on crystal growth with colleagues in academia and at NIST.



Judith Newton, Software Diagnostics and Conformance Testing Division, received the National Committee for Information Technology Standards (NCITS) 2001 Merit Award. Newton was recognized for her dedication as an officer and project editor in the development of data and metadata standards, as well as successful

outreach efforts in emphasizing the importance of metadata standardization to the user community.



Fernando Podio, Convergent Information Systems Division, received recognition from the Federal Laboratory Consortium for Technology Transfer (FLC) for his leadership role in the development of interoperability and data interchange standards and specifications for biometric technologies and the transfer of these specifications to the private sector.

Mike Rubinfeld, Information Access Division, received a 2002 Merit Award from the InterNational Committee for Information Technology Standards (INCITS). The award cites "substantial management accomplishments as the Chairman of the INCITS Technical Committee L3, Coding of Audio, Picture, Multimedia, and Hypermedia Information, that led to key international standards."



Nell Sedransk, Chief, Statistical Engineering Division, was named a Fellow of the American Statistical Association (ASA). Sedransk was recognized "for outstanding statistical leadership in our national metrology program, for consultative contributions in the statistics of oncology, for developing methods to achieve more ethical clinical trials, and for service to the profession."



Ray Snouffer, Computer Security Division, received the prestigious Arthur S. Flemming Award, which is given annually by George Washington University to recognize those who have performed outstanding and meritorious work for the federal government. Snouffer was recognized in the Applied Science category for his sustained contributions and leadership in improving security of commercial cryptographic products and thus the security of federal agencies and private sector organizations. Snouffer heads ITL's Cryptographic Module Validation Program.



Founded in 1901, the National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs:

- the NIST Laboratories, conducting research that advances the nation's technology infrastructure and is needed by U.S. industry to continually improve products and services;
- the Baldrige National Quality Program, which promotes performance excellence among U.S. manufacturers, service companies, educational organizations, and healthcare providers; conducts outreach programs and manages the annual Malcolm Baldrige National Quality Award which recognizes performance excellence and quality achievement;
- the Manufacturing Extension Partnership, a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and
- the Advanced Technology Program, which accelerates the development of innovative technologies for broad national benefit by co-funding R&D partnerships with the private sector.

NIST has an operating budget of about \$839 million and operates in two locations: Gaithersburg, Maryland and Boulder, Colorado. NIST employs about 3,000 scientists, engineers, technicians, and support and administrative personnel. The website is <http://www.nist.gov>.

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

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.*

OPNET is a registered trademark of OPNET Technologies.

Sun, Sun Microsystems, the Sun Logo, Solaris, Java, and Jini are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

**Bluetooth SIG Inc. U.S.A. owns the Bluetooth trademarks.*