Information
Technology
Laboratory

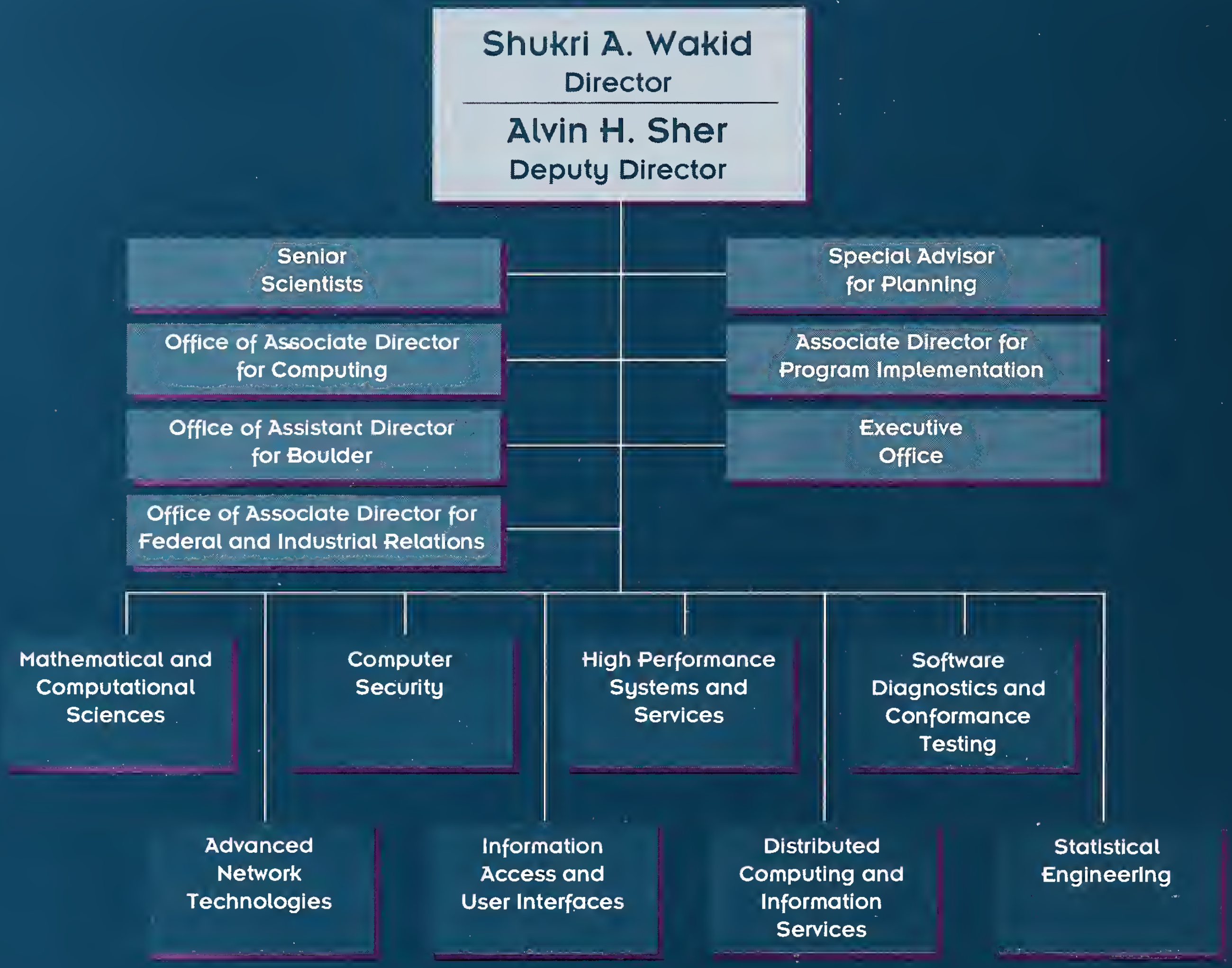
Technical Accomplishments 1996

Working with
industry and
government
to make
information
technology
more usable,
interoperable,
and secure

NISTIR 5938

NIST
tment of Commerce
nology Administration
National Institute of
dards and Technology

Information Technology Laboratory



Shukri A. Wakid
Director

Alvin H. Sher
Deputy Director

Senior Scientists

Special Advisor for Planning

Office of Associate Director for Computing

Associate Director for Program Implementation

Office of Assistant Director for Boulder

Executive Office

Office of Associate Director for Federal and Industrial Relations

Mathematical and Computational Sciences

Advanced Network Technologies

Computer Security

Information Access and User Interfaces

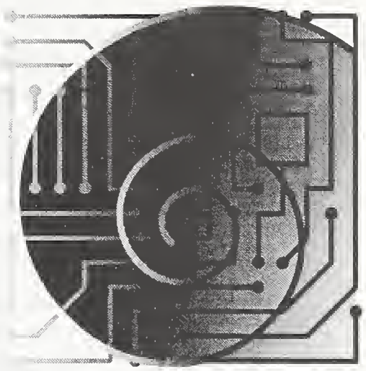
High Performance Systems and Services

Distributed Computing and Information Services

Software Diagnostics and Conformance Testing

Statistical Engineering

Information Technology Laboratory Technical Accomplishments 1996



January 1997

NISTIR 5938

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Information Technology Laboratory
Shukri A. Wakid, Director

DIRECTOR'S FOREWORD

I am pleased to introduce this first annual report of the Information Technology Laboratory (ITL), NIST's newest laboratory organization. NIST provides key elements of the technical infrastructure that enable many industries, including manufacturing, electronics, building, chemical, and information technology, to overcome the barriers to better, faster, and less expensive products. The ITL was formed in 1996 to carry out the NIST mission of promoting U.S. economic growth by working with industry to develop and apply technology, measurements, and standards for information technology.

The new ITL combines and expands the roles of two previous NIST laboratories: the Computer Systems Laboratory and the Computing and Applied Mathematics Laboratory. This new organizational structure enables us to be more responsive to industry and user needs and to be a strong, effective member of the NIST family.

Our program of work concentrates on developing tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. An important aspect is our computational sciences work which focuses on developing the methods and tools needed to formulate and solve difficult mathematical, statistical, and computational problems. ITL's applied mathematicians and statisticians collaborate with their NIST colleagues and industry partners in developing experiment designs and models that help scientists, engineers, and managers work more productively, analyze data more effectively, and understand complex processes. We are also developing test data and reference software to help developers improve the quality of their software. We continue to serve other agencies of the federal government, particularly in computer security, and we continue to help NIST staff members use up-to-date information technology services effectively.

Managing Change

Information technology is a dynamic technology that has sparked the development of many new products and services. Information technology systems are widely distributed throughout the world, and used in almost all businesses and all areas of human endeavor. In just the last few years, tens of millions of people have started to access information across the world through computer networks.

Despite the pervasiveness of information technology in many activities, there are still many barriers to its effective development and use. Information technology encompasses several industry sectors whose boundaries are not rigid, including telecommunications, computing, and consumer electronics, but whose products are expected to be integrated into seamless information networks of the future.

It is not always easy for information technology users to change old ways of doing business or to adapt new methods on a broad scale. Security and interoperability are not guaranteed when new systems are acquired. To exploit the full potential of information technology in the future, it is important to overcome these barriers and to make systems more interoperable, easily usable, scalable, and secure than they are today.

Tests for Information Technology

NIST has traditionally applied its special proficiencies in measurement to developing impartial, neutral, objective tests for physical and chemical properties, and these tests have helped many technology areas to advance. ITL is challenged to bring its expertise to bear on improving the measurement of information technology. In the past, we have had some success in the measurement of the performance of hardware, but test and measurement of software quality are not well understood. The many combinations and possibilities of software lead to unforeseen outcomes and uncertain results.

In this report, you will find summaries of projects to develop tests to accelerate the development of quality products, as well as high-quality, precise advanced standards, early in their development cycles. A few examples include:

Human-machine interface technologies:

- We have developed reference data and benchmark tests to improve the performance of speech recognition systems and enable people to acquire reliable systems that use voice commands for interacting with computers.

- Other reference data sets, evaluation software and proof-of-concept implementations help developers and users of systems that process visual images. Our tools have helped people to evaluate systems used in optical character recognition, fingerprint classification, and face recognition systems.

- Working with government, industry, and academic organizations, we have had a role in improving the accuracy and efficiency of electronic text search and retrieval technology. As the sponsor of the Text REtrieval Conference (TREC), we have been successful in encouraging participants to exchange research results and to transfer new technology from the laboratory into commercial systems.

Tests developed for standards:

- Computer Graphics Metafile (CGM) implementations are being used by the Air Transport Association (ATA) and Aerospace Industries Association (AIA) to test the ability of CGM software to exchange graphics data.

- We have started the development of tests for the Virtual Reality Modeling Language (VRML) to support a forward-looking standard specification developed by the VRML community. We expect that these tests will be used by industry on a voluntary basis early in the development of VRML products.

- Methods developed for evaluating the interoperability of text, graphics, and video applications over Asynchronous Transfer Mode (ATM) networks support the standards activities of the ATM Forum, an industry consortium.

- We are working with the Digital Audio Visual Council (DAVIC), an international consortium for the emerging digital audio-visual applications and services, to develop interoperability tests for digital video products conforming to DAVIC specifications.

Software tools:

- We began distributing S-CHECK (Sensitivity Checker), a portable, scalable tool that we developed for assaying and improving the performances of complex programs. The tool is especially suited for code on parallel systems, where code interactions are common but difficult to evaluate and architectures vary.

Security methods:

- Our proof-of-concept implementation for Role Based Access Control (RBAC) for the World Wide Web provides a tested method of security to limit access to information based on the user's need and the user's role in the organization. These proof-of-concept implementations help product developers by providing software that implements the functions of specifications and augments the written descriptions.

Computational sciences tools:

- Reference data sets are being developed to assure that mathematical and statistical software products are producing accurate results. Developers and users alike will benefit from the reduction of errors and the increased confidence provided.

- Our Guide to Available Mathematical Software provides scientists and engineers with easy access to a large repository of mathematical and statistical software components for use in modeling and analysis projects.

Our Role in Standards

Those familiar with NIST's past information technology activities will remember our work in formal standards organizations and our role in the development of Federal Information Processing Standards (FIPS). To carry out our new agenda for forward- looking standards, we reviewed our standards support activities and reduced efforts in older areas of technology. We continue to support the development of standards, especially in areas where standards will promote international trade and economic growth, and we support the management of the standards process within national and international formal standards-developing groups. We are also working with informal standards groups including industry consortia and professional societies that are developing specifications in advance of the formal standards process.

Previously NIST issued FIPS that adopted voluntary industry standards for federal government use. Agencies are now being directed to use voluntary industry standards as a result of new legislation (Public Law 104-113), thus diminishing the need for FIPS that duplicate voluntary industry standards. We will issue FIPS only where there are compelling federal government requirements. We are reviewing the FIPS that have been issued to assure that the standards are necessary, adequate, and current.

By focusing on tests for forward-looking standards, we believe that we will serve our federal colleagues by improving the quality, at an early stage of development, of the information technology products that they acquire. We are strengthening our technical assistance to users through increased dissemination of electronic information about available standards. We are also planning more extensive help for federal agencies and others in finding and using industry's information technology standards, including the network services being developed by industry to identify standards.

For More Information

I encourage you to explore our Web pages to find out more about our activities; the address is http://www.itl.nist.gov. If you find areas that would be useful in your organization or business, please contact the project leader, group manager, or division chief. We have many ways that we can work with you, and we welcome your inquiries.

Shukri A. Wakid, Director
Information Technology Laboratory
E-mail: itlab@nist.gov

CONTENTS

INTERACTIONS AND ACCOMPLISHMENTS

Overview of the Information Technology Laboratory

Director:	**Shukri Wakid**
Deputy Director:	**Alvin Sher**
Senior Scientists:	**Ron Rehm and Andre Deprit**
Special Advisor for Planning:	**Robert Raybold**
Office of Associate Director for Computing:	**Fred Johnson**
Associate Director for Program Implementation:	**R.J. (Jerry) Linn**
Office of Assistant Director for Boulder:	**Paul Domich**
Executive Office:	**Judith Lyons**
Office of Associate Director for Federal and Industrial Relations:	**Judith Moline**

Information technology (IT) impacts all areas of American life. Within the U.S. economy, about 60 percent of our workers have jobs which depend on the information they generate and receive on advanced information networks. IT has become an essential business tool and has revolutionized the way we conduct the nation's business within the global marketplace. As an enabling technology, IT has become embedded in our household products, entertainment media, and communication networks. While enjoying its many benefits, consumers are challenged to implement and use the ever-changing information technology effectively.

Our New Focus

In 1996, the Information Technology Laboratory (ITL) was established to overcome barriers to usability, scalability, interoperability, and security in information systems and networks. Formed through the consolidation and restructuring of the former Computer Systems Laboratory and Computing and Applied Mathematics Laboratory, ITL seeks to stimulate U.S. economic growth and industrial competitiveness through technical leadership and collaborative research in critical infrastructure technology, including tests, test methods, and forward-looking standards, to promote better development and use of information technology. ITL activities cover a broad range of networking, security, and advanced information technologies, mathematical, statistical and computational sciences, and the operation and modernization of computing and telecommunications facilities within NIST.

The goal of ITL's program is to stimulate the growth and adoption of new technology by helping industry develop better, higher-quality products and helping users evaluate these products. ITL provides key elements of the technical infrastructure to meet industry needs for measurement and standards. Neutral, objective tests are needed to measure interoperability, usability, scalability, and security of systems and to facilitate the implementation of industry-set standards.

Partnership with Industry

ITL works in partnership with industry to strengthen the nation's technology base and to expand its economy. Our primary industry customers include IT providers and users as well as many specialized constituencies such as the mathematical software industry, the medical imagery community, the high speed network and wireless communications industries, security technology developers and vendors, spoken language processing and text retrieval researchers, software and Web browser developers, and the aircraft and construction industries. All of these users of ITL products and services share the problems of overcoming barriers to interoperability, usability, scalability, and security.

An important mechanism for interactions with industry organizations and federal agencies is the Cooperative Research and Development Agreement (CRADA). In 1996, we collaborated with 53 government, industry, and academic institutions through CRADAs to pursue common goals. ITL contributed to the activities of industry groups such as the ATM Forum, the Digital Audio Visual Council (DAVIC), and the Internet Engineering Task Force (IETF) to support interoperability and forward-looking standards. Our ongoing workshop efforts continued – the North American Integrated Services Digital Network (ISDN) Users' Forum (NIUF) and the Federal Wireless Users' Forum (FWUF). Many other informal interactions with government and industry partners involved the sharing of equipment or expertise. These cooperative arrangements benefit all participants through a better understanding of the advantages and barriers to the development and use of information technology.

Our commitment to serving other federal agencies remains strong. Our tests and test methods benefit federal as well as industry customers. Particularly in the area of information security, ITL plays a key role, under the Computer Security Act of 1987, in developing standards and guidelines, and in providing technical assistance to federal departments and agencies in securing their automated information resources.

Office of Federal and Industry Relations

ITL's Office of Federal and Industry Relations serves as a focal point for NIST efforts to provide technical underpinnings for applications of information technology. ITL serves as the U.S. contact for the Global Inventory Project (GIP) and the Electronic Commerce component of the Global Marketplace for Small and Medium Enterprises (SMEs) Project. These pilot projects resulted from the Naples Economic Summit in July 1994, when the G-7 leaders decided to "encourage and promote innovation and the spread of new technologies including, in particular, the development of an open, competitive, and integrated worldwide information infrastructure." Eleven information society pilot project themes were identified which demonstrate the potential of the information society and stimulate its deployment. The key objectives are to support international consensus on common principles governing the need of access to networks and applications and their interoperability and to help create markets for new products and services. Our participation includes the development of Web access to the National Inventory of projects related to the G-7 theme areas and developing and maintaining the registration process and Web site for the Electronic Commerce testbed projects.

ITL continued its support of the Committee on Applications and Technology (CAT) of the President's Information Infrastructure Task Force (IITF). We conducted meetings of the CAT, participated in IITF functions, and assisted the working groups in making their documents available to the public for review. Other activities include maintaining, updating, and revising the NII Virtual Library, developing and maintaining the CAT Web site to make committee and working group information available to the public, and responding to queries about the NII and GII.

In October 1996, ITL cosponsored the Leveraging Cyberspace Conference with the White House and Xerox PARC in Palo Alto, California. We provided technical coordination and established a Web site for the conference. Registration information, conference papers, and comments on those papers were submitted and posted electronically.

Our Organizational Resources

ITL is organized into eight technical divisions: Mathematical and Computational Sciences Division, Advanced Network Technologies Division, Computer Security Division, Information Access and User Interfaces Division, High Performance Systems and Services Division, Distributed Computing and Information Services Division, Software Diagnostics and Conformance Testing Division, and the Statistical Engineering Division. Our professional staff consists of computer scientists, mathematicians, computer specialists, electrical and electronics engineers, and statisticians. Staffing resources in FY 1996 included 408 full-time-equivalent employees of which about 75 percent were professional and technical staff and 25 percent were administrative support personnel. In addition, about 98 research associates, guest scientists, and faculty appointments enhanced our research program.

Funding for ITL programs in FY 1996 consisted of $43.7 million from the NIST Congressional appropriation (STRS), including $11.6 million for the Consolidated Scientific Computing System (Super Computer) and $0.5 million for Technical Competence; $1.7 million from the Advanced Technology Program; and $14.8 million in reimbursable funds, mostly from other federal agencies for direct technical assistance. See the Interactions and Accomplishments section of this report for a complete list of our collaborative interactions.

Our Information Resources

Through a variety of resources, we share information and technology with industry, government, academia, and the public. ITL publishes Federal Information Processing Standards (FIPS) and guidelines; special publications series focusing on information technology, computer security, and ISDN; technical interagency reports on research and tests; a quarterly "ITL" newsletter; and a ITL bulletin series published about eight times a year on topics of interest to the information systems community. See the Interactions and Accomplishments section for a list of publications currently available for sale through the Government Printing Office (GPO) or the National Technical Information Service (NTIS). We also sponsor, cosponsor, and host a variety of conferences and workshops throughout the year, and our staff members address many federal and private organizations.

We welcome your interest in our organization and invite you to visit our Web site at:

http://www.itl.nist.gov

Highlights of our major technical units follow.

MATHEMATICAL AND COMPUTATIONAL SCIENCES DIVISION

Chief: **Paul Boggs**
Group Managers: **James L. Blue, Mathematical Modeling**
Ronald Boisvert, Mathematical Software
Paul Boggs (Acting), Optimization and Computational Geometry
Anastase Nakassis, Compression Algorithms

The Mathematical and Computational Sciences Division provides technical leadership within NIST in modern analytical and computational methods for solving mathematical problems of interest to American industry. This mission is discharged through a program of research and collaboration with technical experts in other NIST divisions, industry, and academia. The scope includes the development and analysis of theoretical descriptions of phenomena (mathematical modeling); the design and analysis of requisite computational methods and experiments; the transformation of these methods into efficient numerical algorithms for high performance computers; the implementation of these methods in high-quality mathematical software; and the distribution of this software to potential clients, both within NIST and to the external community.

The work of the Division is organized into three broad areas: modeling in the physical sciences; software infrastructure for computational science; and compression algorithms.

Mathematical Modeling

Mathematical modeling is an interdisciplinary effort requiring close collaboration between scientists inside and outside the Division. Our researchers cooperate with NIST and other scientists to develop specific mathematical models that capture the essence of the phenomena under study. They analyze the model, propose and develop numerical algorithms, and produce a computer program. The resulting program is run to provide simulations that are compared with experimental results to validate the entire process and to provide the basis for further refinements and enhancements. This process provides more cost-effective, quicker, and better information than experimentation alone. The information allows the NIST and other scientists to gain understanding or to predict behavior of a complex system, and to improve the performance of the system under study.

The customers for our work include our collaborating NIST scientists and engineers, and through these collaborators, industrial scientists and engineers; other customers are the larger community of researchers in computational science and engineering. Our aim is to work on a spectrum of tasks, including engineering and advanced development, and to conduct both short- and long-term research.

Computational materials science continues to be a major thrust of our efforts. Materials science is one of NIST's major areas of expertise, covering a broad range of theoretical, experimental, and computational activities. Long-term mathematical modeling tasks with applications to problems in materials science have been under way by several Division staff members for a number of years; other tasks are relatively new. Notable are long-term efforts in diffuse-interface methods for modeling crystal growth and newer efforts in modeling composite materials and liquid crystals.

We continue to broaden our efforts and to couple more closely with industry. Significant examples include several efforts in modeling the manufacturing process, new work in modeling lasers for use in collision avoidance, and work in using acoustic emissions to diagnose defects in materials.

Software Infrastructure

The goal of the Software Infrastructure for Computational Science project is to improve the environment for computational science through research in fundamental mathematical algorithms and development of well-engineered, general-purpose scientific software. This research combines development and analysis of algorithms for particular mathematical problem domains with the application and advancement of underlying methodologies such as computer arithmetic, parallel computing, languages, software design, user interfaces, documentation, testing, performance evaluation, and information dissemination. The customers for our work in algorithms and in the dissemination of software and related information include NIST scientists and engineers as well as the science and engineering community at large. Our work in testing and evaluation methodology is of particular interest to the math software research community, as well as to developers of math software products in the commercial sector.

We initiated a new joint project with the Statistical Engineering Division on Tools for Evaluating Mathematical and Statistical Software. Particular tasks in the areas of numerical linear algebra, special function evaluation, and statistical software are in process. The Matrix Market, a visual database of test data for large sparse matrix algorithms, is the first visible output of this project. The database has already generated positive feedback on its usefulness to the research community; collaborations began with users of sparse matrix technology, such as the Boeing Company, to include additional large-scale test data in the collection. We also started work on the development of a Web-based software testing service for special functions.

We made significant progress in applying object-oriented software design to improve portability and reuse of mathematical software. Several demonstration software packages for core linear algebra operations in C++ were released and are seeing widespread attention. This work spawned interest in the development of a standardized set of basic linear algebra software for elementary sparse matrix operations. We collaborate with Cray Research on this project.

We initiated several projects to develop algorithms, software, and tools for distributed parallel scientific computing. Our scalar processors algorithms exemplified by our highly successful MGGHAT package, which solves partial differential equations using high order hierarchical-basis adaptive multigrid methods, proved extremely effective. Moving computations such as these to distributed parallel architectures is difficult due to complex load balancing and data communications issues. This year, we completed the prototype of a new software package named PHAML which parallelizes such computations based upon new multigrid-based domain decomposition and refinement-tree-based load balancing strategies. We continued to contribute to the development of software development tools, such as the Parallel Applications Development Environment (PADE), a joint project with the High Performance Systems and Services Division and the NIST Physics Laboratory. We also provided specialized support for use of the IBM SP2 parallel computer with educational materials and utilities such as xllcreate.

The Guide to Available Mathematical Software (GAMS) continues to see high use by the science and engineering community. Since its inception in 1994, the server has satisfied more than three million requests. Digital's AltaVista search engine identifies more than 3,000 external Web pages that link to the GAMS server, and the McKinley Group (a commercial venture that rates Web pages for presentation and content) awarded GAMS its four-star (highest) rating. We investigated new technologies for increasing the usefulness of scientific software repositories, and this year we released a prototype of HotGAMS!, a Java-enabled GAMS client which provides a new interface which is more capable, portable, and efficient.

Compression Algorithms

The naive representations of information, including an image represented as a set of pixels or human thought written in languages based on alphabets, are often highly redundant; in addition, they contain information that the intended recipient cannot process, e.g., recording frequencies outside the human audible spectrum. Such representations can be compressed through information encodings that reduce redundancy or remove unneeded accuracy. In some instances, further reductions can be obtained by introducing small, inconsequential changes in the information to be encoded, i.e., distortion or pixel values that differ from the original ones. This project currently focuses on image compression and seeks to develop, study, and assess both lossless and lossy compression algorithms.

This year we developed tools for the selection of optimal orthogonal wavelets (biorthogonal wavelet generator), investigated new combinations of known compression techniques (development of code-books applicable to multiple-image classes), and initiated joint inquiries with industrial partners into the services needed to support effective video delivery. Specific topics included adaptations of forward error correction codes that exploit the structure of the encoded video, the fact that the constituent parts of the signal are not equally important, and image estimation techniques to reduce the impact of signal loss.

ADVANCED NETWORK TECHNOLOGIES DIVISION

Chief: **Kevin Mills**
Acting Chief: **Craig Hunt**
Group Managers: **David Su, High Speed Network Technologies**
Craig Hunt (Acting), Wireless Network Technologies
Jean-Philippe Favreau, Multimedia & Digital Video Technologies
Craig Hunt, Internetworking Technologies

Information technology trends indicate an ongoing move toward a future of universal, continuous access to information. Three barriers to realizing this future are interoperability problems, scaling problems, and security problems. The Advanced Network Technologies Division concentrates primarily on overcoming the first two barriers and on eliminating their detrimental effect on the development of a global network infrastructure. Our contributions to overcoming these barriers are focused on developing test methods, such as testbeds and reference implementations for interoperability testing, and simulation analysis of protocol interactions and scaling limits. Each group's projects and accomplishments are described below.

High Speed Network Technologies

The High Speed Network Technologies Group continued its leadership role in developing test suites for Asynchronous Transfer Mode (ATM) network protocols, specifically in the Testing Working Group of the ATM Forum in developing abstract test suites (ATS) for conformance and interoperability testing of the ATM network protocols. Our efforts concentrate on testing of call control signaling, routing, and traffic management protocols. The ATM Forum is an industry standards consortium that is developing standards for high speed digital technology for networks.

ATM is not the only high speed technology being developed. The industry standards group IEEE 802.14 is developing protocols for high speed bi-directional data communication over Hybrid Fiber/Coaxial (HFC) networks currently being used or deployed by the Cable TV (CATV) industry. The 802.14 group is working on a draft specification that will include protocols for the Physical Media (PHY) and Medium Access Control (MAC) protocol layers. Many MAC protocol proposals have been submitted to the 802.14 working group by CATV equipment vendors.

As an unbiased third party and at the invitation of the IEEE group, ITL participated in the evaluation of these MAC proposals. Since joining the group in February 1996, we produced five reports to the group based on the results of computer simulations conducted in our laboratory. The subjects of these reports included performance comparison of MAC proposals, analysis of MAC frame formats, comparison of contention resolution algorithms, and evaluation of bandwidth allocation methods. These reports helped the standards group achieve several important agreements in arriving at a final MAC protocol.

A major revolution in information technology is the increased use of integrated services involving voice, data, and video over networks. Digital video applications are expected to be the major sources of network traffic in the future. To foster interoperability of emerging digital video products and services, we developed an interoperability test laboratory that enables vendors to test for interoperability of their products against our standards-conforming implementations as well as products from other vendors.

Video-on-Demand (VoD) service is the first digital video application that we are testing. We developed a prototype VoD system based on the specifications of the Digital Audio Visual Council (DAVIC), an international consortium to develop implementation agreements for digital video applications. We demonstrated the prototype system in the DAVIC interoperability event held in parallel with the 13th DAVIC meeting in New York in June 1996, hosted by Columbia University. A total of eight organizations from Europe, Asia, and North America participated in the event, interconnecting components such as video servers, set-top-units (STUs), and applications over an ATM network. In this event, our VoD system interoperated with systems from NTT and GCL in Japan, CSELT in Italy, and Columbia University. Our efforts continue in two major areas: the development of a VoD reference implementation and the development of a VoD interoperability test suite. The test suite will be submitted to DAVIC for inclusion in its specifications.

Wireless Technologies

Our Wireless Technologies Group continued to make progress in 1996. We completed experimental work with NASA's Advanced Communication Technology Satellite (ACTS). The test data generated was used by the National Telecommunications and Information Administration (NTIA) to produce a report on the viability of advanced satellites for emergency communications. This viability was demonstrated in a live, multimedia video conference between a member of the Wireless Technologies Group and participants at MITRE, Comsat, and NTIA.

Using a voice recognition system, we built a tool to analyze the quality of voice after it has been encoded, transmitted over a wireless system, and decoded. If this technique proves valid, it will be the first automated tool for measuring voice intelligibility. The tool could prove valuable to people developing voice encoding systems or people evaluating the impact of noise on these systems.

Multimedia and Digital Video

The Multimedia and Digital Video Group works with industry to promote the development of cost-effective, interoperable, distributed multimedia applications and to enable the development of digital video technologies for broadcast, interactive television, video-on-demand, and video conferencing. The Group focuses on three areas: measurement techniques for characterization of distributed multimedia technologies and digital video devices and services; techniques for integrating multimedia services with network technologies; and industry-driven standards for multimedia technologies and digital video devices and services. The video-on-demand work is done in collaboration with the High Speed Network Technologies Group and is reported above.

In collaboration with MITRE and Carnegie Mellon University (CMU), the Group works on the Defense Advanced Research Program Agency (DARPA) Intelligent Collaboration and Visualization Program (IC&V) program. The goal is to identify and apply an evaluation and benchmarking approach to the collaboration infrastructure and applications that will be developed with DARPA funding.

We continued our work with the International Telecommunications Union (ITU) recommendations on transmission protocols for multimedia data. These standards deal with transmitting data in various formats (i.e., audio, video, data) in an efficient, secure, and flexible manner. During FY 96, the activity resulted in the development of a convergence layer protocol that supports multicasting and fits between ITU T.120 specifications and the underlying transport protocol.

The Group established a program in multimedia interoperability working with and supporting the International Multimedia Teleconferencing Consortium (IMTC). Initial areas of collaboration included interoperability testing of ITU T.120, "Transmission Protocols for Multipoint Data," and ITU H.324 "Visual Telephone Terminals over GSTN." Other interactions included aiding in the development of an interoperability test management plan and interoperability test suites for both T.120 and H.324, hosting interoperability testing events and vendors in our laboratory facility, providing technical support personnel for testing in the laboratory, aiding in the publishing of testing results, and participating in remote demonstrations by making the laboratory available to IMTC members as a remote site.

Internetworking Technologies

Division personnel actively participate in the design, development, testing, and demonstration of next generation internetworking technology. These activities focus on current efforts within the Internet Engineering Task Force (IETF) to add major new functionality to the Internet Protocol Suite (IPS). Our efforts concentrated on three major technical areas that hold promise for the most significant improvements to the capabilities of the IPS infrastructure: network security protocols, integrated services, and the next generation internetwork protocol.

In the area of network security protocol development, staff members took a leadership role in the IETF and vendor community in the design and prototype implementation of internetwork layer security protocols, known as IPSEC. Through a cooperative engineering effort with the National Security Agency (NSA), we developed a very successful public domain reference implementation of the IPSEC protocols for authentication and privacy. The NIST prototype implementation was tested successfully in two public interoperability trials and in numerous bilateral testing sessions with emerging vendor implementations. Through the NSA Technology Transfer Program, the NIST prototype implementation has been distributed to more than 20 organizations in the U.S. and abroad.

In addition to prototype development, ITL contributed to the design of the IETF IPSEC protocol. Two specifications of authentication transforms with replay prevention mechanisms, authored by our staff, are advancing towards Draft Standard status within the IETF.

In the area of integrated services, Division staff contributed to the IETF effort to add support for real-time, quality of service (QoS) controlled capabilities to the existing Internet Protocol Suite (IPS). Our efforts focused on two critical components of this effort: the Resource Reservation Protocol (RSVP) and Real Time Transport Protocol (RTP). Division staff constructed a multi-vendor testbed for experimentation with early implementations of RSVP, RTP, and emerging applications demonstrating QoS capabilities. We are also developing test and instrumentation tools to foster experimentation and early deployment of IPS integrated services protocols.

ITL also contributed to the IETF's effort to design and deploy the next generation internetwork protocol: IP version 6 (IPv6). We deployed an advanced multi-vendor testbed facility consisting of very early vendor and academic implementations of IPv6 and supporting network services, tools, and applications. The NIST testbed is a key component in the "6-Bone," an international virtual IPv6 backbone that connects IPv6 testbeds in the U.S., Europe, and Asia. The NIST testbed serves as a primary gateway between U.S. and European components of the 6-Bone. In addition to the testbed activity, we added to the security capabilities of public domain IPv6 implementations.

Computer Security Division

Chief: **Stuart Katzke**
Group Managers: **Miles Smid, Security Technology**
Tim Grance, Systems and Network Security

The mission of the Computer Security Division is to ensure the availability of technology and measures to protect information integrity, availability, and confidentiality in computer systems and networks. The success of electronic commerce and the widespread use of the Internet depends to a great extent on the degree to which the users of this information technology can trust it to protect valuable, critical, and confidential information. The goal of ITL's Computer Security program is to meet the security technology, standards, and testing needs of both industry and government. Our Computer Security program has six primary focus areas:

- **Cryptographic Technology and Applications** - to help establish common cryptographic security technology (algorithms, functionality, and interfaces) to support information technology (IT) systems and networks.
- **Advanced Authentication** - to develop a common authentication architecture that permits secure (trusted) identification and authentication across networks and systems.
- **Public Key Infrastructure** - to enable establishment of a nationwide (ultimately, global) infrastructure for managing public key certificates needed to facilitate data integrity, authentication, access control, non-repudiation, and data confidentiality services in global applications.
- **Internetworking Security** - to ensure that incident prevention, detection, reaction, and information sharing capabilities are embedded in the technical and operational fabric of IT systems and networks.
- **Criteria and Assurance** - to ensure the availability of affordable, reliable, and trustworthy security technology, systems, and products for use in IT systems and networks.
- **Security Management and Support** - to provide direct support and other guidance to ensure effective use and management of security technology. Activities include the National Information Systems Security Conference and a number of special projects.

The following are highlights of the activities and accomplishments of the Computer Security program in FY 1996.

Cryptographic Technology and Applications

One of the keys to the widespread use of cryptographic protection in application systems is a commonly accepted set of application programming interfaces (APIs) that can be used by programmers to call on cryptographic services. ITL led efforts to develop as set of such APIs, known as the NIST Cryptographic Application Program Interfaces (CAPIs), and this API set has been used as the basis for CAPI development in voluntary industry standards bodies.

We completed the commercialization of the Cryptographic Module Validation Program by accrediting laboratories to perform cryptographic module validations in accordance with Federal Information Processing Standard (FIPS) 140-1, *Security Requirements for Cryptographic Modules.* This is a joint effort with Canada and currently involves three laboratories accredited to perform FIPS 140-1 testing.

In anticipation of future needs for high-quality cryptography, the Division initiated planning in 1996 for the development of new advanced cryptographic algorithm standards, for encryption, digital signatures, and key exchange.

As key escrow program manager, we provided technical oversight of the key production and escrowing process. In accordance with a presidential directive, NIST serves as secretariat for a newly formed Technical Advisory Committee for the development of a Federal Key Management Infrastructure. This advisory committee is designed to obtain private-sector assistance in the development of needed cryptographic key management services for the government.

Advanced Authentication Technology

Efficient and secure authentication of users and other entities in a computer system and network has long been critical to effective information security. NIST has led efforts to promote methods other than traditional re-usable passwords for authentication purposes. In the open network environment of the Internet, these alternatives to passwords are crucial, since any password, once used, can no longer be assumed to be secure.

NIST completed work on a FIPS to provide a standard protocol for the mutual authentication of entities (e.g., users, hosts, servers, etc.) in a network environment. This standard will provide for a higher level of assurance and trust among cooperating entities in the growing global Internet.

Public Key Infrastructure (PKI)

Without a common infrastructure to support the issuance, management, distribution, and verification of public key certificates, the full benefits of cryptographic services will not be achievable. NIST is leading efforts to develop such a public key infrastructure (PKI). Many of the U.S. Government's PKI activities are coordinated through the Federal PKI Steering Committee. NIST chairs the Technical Working Group of the steering committee and hosted meetings of the committee itself. The working group produced several technical documents on PKI issues, including an overall PKI Concept of Operations and PKI architectural and policy analyses.

We completed work on the development of digital signature mechanisms (based on the Federal Digital Signature and Secure Hash Algorithms, DSA and SHA) for a NIST Automated Purchase Order System. These mechanisms help ensure the integrity of purchase transactions initiated through the system.

We received funding under the Government Information Technology Services (GITS) innovation fund program to develop a prototype root certificate authority (CA) as a central component in a PKI. This project is scheduled for completion in FY 1997.

Twelve private-sector firms joined ITL in a PKI interoperability effort through the Cooperative Research and Development Agreement (CRADA) process. The first step in this project was the development, review, and issuance of a Minimum Interoperability Specification for PKI Components, scheduled for completion in early FY 1997.

Internetworking Security

Our Division actively participates in the development of security mechanisms in the future Internet protocol standards (collectively known as IPv6 – Internet Protocol Version 6).

Traditional permission-based and privilege-based access control mechanisms, while relatively simple in principle, are often difficult to implement and maintain in practice, primarily because they focus on the computer system rather on the person and the job to be done. We developed a new type of access control model, based on defining access in terms of the roles to be performed. Role Based Access Control (RBAC) has been demonstrated through a World Wide Web (WWW) proof-of-concept model. Work on the RBAC model will continue in FY 1997.

NIST co-chairs the Privacy and Security Working Group of the Federal Networking Council (FNC), a multi-agency effort to coordinate the Internet research efforts of the federal government community. The Group was awarded a GITS innovation fund grant for a project on Collaborations in Internet Security (CIS). This project will bring together Internet security projects and testbeds from several agencies to facilitate sharing of technologies and effort.

Criteria and Assurance

We initiated efforts for and increased focus on security testing through the planned establishment of a national Testing Competency Center at NIST. This Center, when fully funded and operational, will provide a common point for the development of security testing criteria (including both test methods and testing laboratory requirements). By ensuring the availability of security testing facilities and services, NIST will help ensure the availability of security products and services that can be used with confidence by government and private-sector organizations.

NIST has been involved in an international effort to develop a set of Common Criteria (CC) for the testing and evaluation of security systems and products. The Common Criteria v1.0 was completed and released for public review. The CC is designed to provide the basis for commercial testing of products and for international mutual recognition of test certifications, thus providing for an expanded market for high-quality, trusted security products and systems.

Security Management and Support

Information technology security is much more than technology. Indeed, effective security protection requires a comprehensive and cohesive set of physical, technical, and administrative measures. We have long provided both private-sector and government organizations with authoritative guidance for the protection of IT systems.

We have been actively involved in the development of computer security incident response capabilities. NIST was one of the founding members of the Forum of Incident Response and Security Teams (FIRST), an international consortium of incident response teams. To further the incident response efforts within the federal government, NIST received a GITS innovation fund grant of $2 million to develop an incident response capability for federal agencies. The effort, named the Federal Computer Incident Response Capability (FedCIRC), will provide incident response services at various levels on a subscription basis for federal agencies.

To provide comprehensive, up-to-date guidance on IT security, NIST issued Special Publication 800-12, *Introduction to Computer Security: The NIST Handbook*. The handbook provides managers with a cohesive, up-to-date overview of all key aspects of computer security, including basic objectives and controls and references to additional detailed publications and guidance.

As part of its overall effort to provide both general and specific guidance for the protection of computer systems and networks, we developed and issued NIST Special Publication 800-14, *Generally Accepted System Security Principles and Practices (GSSPs)*. This document provides a high-level set of basic principles (based in part on internationally recognized guidance) that apply to all computer and network systems and that should be implemented through technical, physical, and administrative measures appropriate to the system(s) in question.

To facilitate access to NIST publications and guidance, as well as a wide variety of other sources of computer security information, we maintain the Computer Security Resource Clearinghouse (CSRC). The CSRC is a World Wide Web (WWW) site containing references to or electronic copies of many NIST computer security documents as well as links to many other valuable resources available on the Web. The address of the CSRC is ***http://csrc.nist.gov***.

NIST cosponsors, with the National Security Agency, the annual National Information Systems Security Conference (formerly the National Computer Security Conference) in Baltimore, Maryland. The conference, one of the largest of its kind, provides a forum for the government, commercial, and academic communities to come together to discuss the latest developments in information security technology. In addition, NIST serves as secretariat for advisory committees and other groups designed to further discussion, cooperation, and coordination among the key communities in the information security field. Two notable groups are the Computer Systems Security and Privacy Advisory Board (CSSPAB), established by the Computer Security Act of 1987, and the Federal Computer Security Program Managers Forum.

INFORMATION ACCESS AND USER INTERFACES DIVISION

Chief (Acting): **Shukri Wakid**
Group Managers: **David Pallett, Spoken Natural Language Processing**
Donna Harman, Natural Language Processing and Information Retrieval
Charles Wilson, Visual Image Processing
Sharon Laskowski, Visualization and Virtual Reality

The mission of the Information Access and User Interfaces Division is to accelerate the development of technologies that allow intuitive, efficient access, manipulation, and exchange of complex information by facilitating the creation of measurement methods and standards. These technologies include the digitization and representation of multimedia data and the use of spoken and written natural language and visual interactive modalities for search and presentation of that information. Through collaboration with industry, academia, and government, the Division coordinates and provides evaluation methodologies, test suites and corpora, prototypes, workshops, and standards and guidelines to enable faster transition into the commercial marketplace.

Spoken Natural Language Processing

ITL advances the state of the art of spoken language processing (speech recognition and understanding) so that spoken language may serve as an alternative modality for the human-computer interface. Our researchers provide reference materials (speech corpora) used by the research and development community, develop test procedures and coordinating communitywide benchmark tests, and build prototype systems. The benchmark tests serve to document progress in selected prototypical spoken language applications domains.

Researchers work closely with industry and other federal agencies to further the development of prototype systems that will permit access to information technology and large knowledge bases using spoken language. These prototype systems contribute to the development of technologies that will permit future access to information services using spoken natural language technologies over the telecommunications network, without requiring reliance on either keyboards or display screens.

ITL has worked with the Defense Advanced Research Projects Agency (DARPA) spoken language community since 1984, filling a key role in the development and use of speech corpora (databases of speech, transcriptions, and related materials) by this research community. These reference corpora are used for system development and test purposes. Approximately 200 CD-ROMs have been produced by ITL to disseminate these speech corpora throughout the worldwide speech research community, including copies distributed through the National Technical Information Service (NTIS) and the University of Pennsylvania's Linguistic Data Consortium (LDC).

Benchmark tests, which we have implemented within this community since 1987, are used to track technology development for several speech technologies, including speech recognition and understanding, several spotting technologies, and most recently, language identification. The scope of speech recognition technologies under development and test within our community now includes recognition of conversational telephone-channel speech in several foreign languages, including Spanish, Mandarin, and Japanese. In FY 1996, as in prior years, we implemented benchmark tests for the DARPA Human Language Systems Program and for the Department of Defense. These tests involved a number of "volunteers," research organizations not under contract to the sponsors. Participants included AT&T Bell Laboratories, BBN Systems and Technologies (BBN), Boston University, Cambridge University Engineering Department (England), Carnegie Mellon University (CMU), Centre de Recherche Informatique de Montreal (Canada), Dragon Systems, IBM T.J. Watson Research Labs (IBM), International Computer Science Institute, ITT, Centre National de la Recherche Scientifique-Laboratoire d'Informatique pour la Mecanique et les Sciences de l'Inginieur (LIMSI) (France), MIT Lincoln Laboratory, MIT Laboratory for Computer Science, MITRE Corporation, New York University, Oregon Graduate Institute, Unisys, University of Karlsruhe, (Germany), Philips GmbH Research Laboratories (Germany), Sanders-Lockheed, and SRI International.

The first "dry run" benchmark tests were successfully conducted at four DARPA contractor's sites (BBN, CMU, Dragon Systems, and IBM), using broadcast data processed by ITL in coordination with the University of Pennsylvania's Linguistic Data Consortium. ITL advocated the use of radio broadcast materials, derived from the Public Radio International "Marketplace" program involving financial news, for these benchmark tests of large vocabulary, speaker-independent, continuous speech recognition technology. The scope of the task was broadened to include "news broadcast" materials derived from both radio and television news broadcasts, and we prepared additional test materials. Preliminary tests on the broadened "broadcast news" task were recently conducted at nine sites. ITL serves as implementor of these benchmark tests, and is responsible for both preparation of the test materials and implementation of all scoring protocols and preparation of summary reports.

We also participated in software sharing efforts involving Cambridge University and Carnegie Mellon University. Our speech recognition test scoring software is widely used internationally. This approach to benchmark testing was adopted for use in the European Union (EU)'s SQALE Program, a multilingual speech recognition project involving the TNO Institute for Perception in the Netherlands, Cambridge University, LIMSI, and Philips GmbH Research Laboratories.

In another ARPA-sponsored project, we worked with Carnegie Mellon University in porting spoken language understanding technology and built a prototype system for this domain. The prototype system provides a spoken natural language interface to electronic libraries, as a specific example of spoken language interfaces to information services. Recent enhancements to the system include automated access to the Montgomery County (Maryland) Public Library collection and to a Web bookseller to look up specific books to determine availability for public library patrons or for purchase.

Natural Language Processing and Information Retrieval

This Group promotes the use of more effective and efficient techniques for manipulating unstructured textual information, especially the browsing, searching, and presentation of that information. Some of the projects in 1996 are continuations of previous work, but we initiated several new projects.

We continued our very successful Text REtrieval Conferences (TRECs), cosponsored by ITL and DARPA. This conference attracts international participation from information retrieval researchers in industry, academia, and government. The conference has grown from 25 systems in 1992 to 38 systems in 1996, and serves as a major technology-transfer mechanism. The participating groups work with large (ITL-built) test collections, use the same evaluation procedures, and meet for a three-day workshop to compare techniques and results. New for 1996 were investigations into retrieval in Chinese and Spanish, and evaluation of systems using input text produced by degraded optical character recognition (OCR).

Another project is the continued development of the NIST prototype retrieval system, the ZPRISE system. This prototype is based on statistical ranking techniques and was initially developed to prove the effectiveness of these techniques in searching large collections of unstructured text. Earlier work extended this prototype to include a Z39.50-1994 UNIX client and server; this was released as public domain software in July 1995. The goals are to increase our understanding of the Z39.50 standard and our ability to influence and encourage its development and use; to promote the availability of information retrieval services by publishing source code for a working Z39.50 client/server; and to provide an enhanced, user-friendly version of our PRISE application within a Z39.50 interface. Over 80 research and commercial groups worldwide have requested this software. Currently a second release of ZPRISE is under development that will enhance the 1995 version using results from research conducted during 1996. This includes query expansion tools using relevance feedback and a redesigned client based on usability testing done in May 1996.

We are pursuing two projects in conjunction with the Social Security Administration (SSA). The first is consultation and design of usability testing for a pilot search system based on ITL's prototype EAMATE system. This pilot is currently being installed to search 210 gigabytes of earnings records and is scheduled for user testing in the spring of 1997. The second project is a new prototype called HyperIndexer, which is being built to explore the use of automatically built links to access SSA manuals.

We initiated a new feasibility project to investigate methods of building "intelligent" database access systems that can access both textual and non-textual data. This project will be demonstrated for several domains during 1997. Additionally, the Group jointly ran ITL's first usability engineering (UE) symposium (116 attendees) which brought industry and government together to promote the use of UE techniques and to exchange strategies for achieving effectiveness and efficiency in computer systems. Follow-on meetings will focus on usability measurement and methods.

Visual Image Processing

ITL supports the technology of image recognition in government and industry by developing new image recognition methods, developing techniques for the evaluation of existing methods, and providing technology transfer to the commercial imaging and document conversion industry.

In cooperation with the Federal Bureau of lnvestigation (FBI), we are developing methods for evaluation of optical information processing for face and fingerprint applications and mugshot standards. The goal of the optical information processing project is to develop the metrology needed to industrialize optical information processing using a real commercial application as a testbed. ln the mugshot standards project, we seek to develop a standard method for acquiring electronic mugshots which is usable at all levels of law enforcement.

The FBl funded the initial phase of the optical information processing project, which has allowed us to explore the feasibility of optical methods of image storage, 3-D holography, and combining optical correlation and neural networks for fingerprint matching. These efforts showed that properly characterized 3-D analog holographic memory has capabilities for image storage which is sufficient to support various correlation methods of pattern recognition. We also demonstrated that a combination of local optical correlation and neural network matching can be used to provide the first advance on minutia matching in 20 years. If properly combined, these methods should allow a new class of optical pattern matching system to be developed.

The expertise developed in the initial phase of this project allowed us to specify high-impact commercial applications which could use this technology. This is real-time fingerprint matching for user verification for financial use, credit, and lnternet security. The Financial Services Technology Consortium is interested in the first application and several small companies are actively pursuing the network access market. ln both of these applications, fingerprint matching, retinal scan matching, and face recognition have all been suggested. The projected costs, the input device, and user inconvenience make fingerprint and face more attractive candidates than retinal scanning. At the present state of the technology, fingerprint matching can provide much higher levels of security. In samples of a few thousand, look-a-like faces can usually be found. ln 30 millicn fingerprint samples, no matches have been found between different individuals.

ln November 1996, the Visual Image Processing Group released a second version of our public domain OCR system. The new version is approximately twice as fast, has half the errors, and uses half the memory of the previous version of the system. The recognition system processes the Handwriting Sample Forms distributed with NIST Special Database 19. The system reads handprinted fields containing digits, lowercase letters, uppercase letters, and reads a text paragraph containing the Preamble to the U.S. Constitution. Seven hundred copies of the first version were distributed prior to the second release. The release of this system completed our work on form-based OCR systems.

Our Group will begin work in FY 1997 on cost-effective document conversion technology in cooperation with the National Security Agency (NSA). Commercial off-the-shelf (COTS) technology for many areas of document conversion is being widely used for tasks such as universal library conversion but this technology does not address the need for large-scale, timely conversion of low-quality documents and the impact of this type of conversion on information retrieval. ITL plans to develop the technology needed to apply the evaluation conference concept to the document conversion problem. Conferences will be held to define and focus both commercial and academic research efforts on specific problem areas, to exchange research ideas, and to identify areas requiring future work.

Initially, ITL will use 67,000 pages of the *Federal Register* (the entire year 1994) which have full typesetting instructions and paper documents. This allows the effect of OCR on ideal images generated by typesetting the text to be compared to real images of scanned paper and allows the effect of various image degradation models to be compared with the OCR of real images. Initially, this comparison will take place in a subset of the data in the 1996 TREC Conference.

Visualization and Virtual Reality

Information visualization is receiving much attention within the human-computer interaction and graphics research communities because it holds much promise as a technology that will enable the display and exploration of large, complex information spaces. ITL's Visualization and Virtual Reality Group was formed in FY 1996 to advance the state of the art in information visualization and virtual environment technology through the development of evaluation methodologies and metrics that address both the usability and scalability of three-dimensional visualization approaches and through the creation of proof-of-concept prototypes, standard reference data sets, and formats for simplifying the integration of visualization tools with applications.

In FY 1996, we developed several three-dimensional interfaces to the NIST PRISE information retrieval system to support easier access to document collections. These systems will form the basis of experiments to support the evaluation of the effectiveness of such interfaces. ITL continues to pursue opportunities within the information retrieval and digital library communities to supply appropriate evaluation methodologies and guidelines that will leverage the technology to support innovative uses of visual displays of information for information retrieval.

A second project, begun two years ago, centers around investigating the appropriateness of virtual environments and the Virtual Reality Modeling Language (VRML) for manufacturing applications. The project is affiliated with users and developers through a collaboration with NIST's Manufacturing Engineering Laboratory and the Systems Integration for Manufacturing Applications program. The goal is to assist the manufacturing community in exploring how visualization can improve the manufacturing process. This led to the software modeling of factory floor assembly lines, machine tools, and parts with all associated multimedia information as a virtual environment in VRML. The VIM (Visual Interface for Manufacturing) prototype was constructed in FY 1996 and will support an investigation of the feasibility and usability of Web-based virtual environments for modeling manufacturing processes. We also acquired data from the Consumer Product Safety Commission consisting of detailed infant and child measurements. This database will be placed into electronic form and converted to VRML models of children via a human body motion simulation package.

If successful, this research will be used to construct a standard reference database giving manufacturers easy, platform-independent access to data critical to the testing of the safety of their products.

In late FY 1996, ITL began a collaboration with researchers who have formed a group to develop large datasets to support the visualization and data mining community. The goal is to create large, public datasets in which researchers can experiment with and evaluate the effectiveness of visualization techniques to support information exploration. This is similar to efforts in the machine learning community, but with an emphasis on very large, timely datasets. Also in late FY 1996, we initiated work under the DARPA Intelligent Collaboration and Visualization Program. As part of an evaluation effort designed to provide evaluation tools for DARPA-funded researchers, ITL is addressing the difficult question of how to measure and evaluate collaborative systems by providing metrics and dynamic evaluation and instrumentation tools. We also began internal experimentation with a collaborative tool that is designed to support the standards authoring and commenting process.

HIGH PERFORMANCE SYSTEMS AND SERVICES DIVISION

Chief: **Dean Collins**
Group Managers: **Gordon Lyon, Scalable Parallel Systems and Applications**
Jack Newmeyer, High Performance Systems Usage
John Antonishek, Network and Telecommunications Systems

Research and development of innovative measurement standards, test methods, and testbed design are crucial to the deployment of technologies. The Division assesses the functional capabilities, interoperability, and operational characteristics of high performance systems and provides high performance computing services to NIST scientists.

MultiKron, a VLSI Tool for Performance Measurement

The NIST-developed MultiKron series of VLSI instrumentation chips and interface boards are measurement tools that promote the development of high performance computing and flexible, scalable systems. The NIST chips measure the performance of parallel processors and workstations on high speed networks by recording events triggered either by software memory writes or the transition of hardware signals. The chips can either timestamp captured data and send it over a collection network or use it to control counters and clocks aboard the chip. The resulting accurate measurements permit researchers to understand the source of performance bottlenecks and therefore learn how to scale their system designs upwards without significantly perturbing the system under measurement.

The current instrumentation consists of the MultiKron_II and the MultiKron_vc chips, and their associated tool kits. The chips are designed to be memory mapped to the local processor(s), via the memory or I/O bus. The MultiKron_II provides both event tracing and 16 performance counters, while the MultiKron_vc provides only performance counters, but thousands of them. The MultiKron tool kits are printed circuit boards (PCBs) that contain a MultiKron chip, interface logic to a standard I/O bus (currently VME, Sbus, and PCI), logic for support and management of the MultiKron, and two data storage schemes; a local, dedicated memory on the PCB or a cable to another machine. These tool kits, distributed free of charge, are designed so that experimenters can plug in the PCB, install its support software, and begin to integrate performance measurement into their experiments.

MultiKron technology is being used by U.S.-based computer companies including Intel, Alliant TechSystems (Mukiteo, Washington), and Tera Computer Co. (Seattle, Washington). Intel extracted and implemented a functional subset of MultiKron into their Paragon supercomputer. Alliant TechSystems has used MultiKron concepts in a commercial "UniKron" gate programmable instrumentation for industrial process lines. Tera, a new supercomputer company, has incorporated MultiKron concepts in their machine, which is currently in Beta testing.

Advanced User Interfaces for Supercomputing Applications -WebSubmit

WebSubmit was developed as an Intranet application tool that provides an advanced Web page interface to supercomputing applications. It differs from other Web applications because it allows interaction with a user's data files and directories on the target supercomputer. These interactions include reading and writing of the user's data files, functions not normally allowed via a Web page. The advantage of a Web-based interface is that it is hardware and software independent; it is only dependent on whatever Web browser the user has available.

The current WebSubmit implementation is for an IBM SP2 supercomputer and has interfaces to the LoadLeveler job scheduling software; Gaussian 94, a molecular dynamics program; functions to monitor jobs and files on an SP2; and file transfers. All the Web pages are dynamically generated with CGI scripts written in Tcl. The Tcl code is modular, making the addition of new interfaces very easy, and simple to customize for a particular SP2 site.

Future plans for WebSubmit include investigating the use of Java and JavaScript for client-side Web page generation and interaction; using the Virtual Reality Modeling Language (VRML) for visualization of Gaussian 94 data; creating a LoadLeveler interface that hides the details of the LoadLeveler and concentrates on the type of problem the user wants to run; and improving the security model of WebSubmit to prevent unauthorized use.

S-CHECK, a Tool for Tuning Complex Programs

ITL began distributing a novel tool, S-Check (Sensitivity Checker), for assaying and improving performances of programs. The tool is especially suited for code on parallel systems, where code interactions are common but difficult to evaluate and architectures vary a lot. Code performance interactions are not handled by conventional profiler tools, but S-Check can do this; it detects and quantifies performance interaction strength among suspected code components. S-Check also enjoys the advantage of being portable and scalable.

As a tool, S-Check provides a powerful mix of industrial process control and computer automation. Current versions handle C language programs. S-Check provides capabilities well beyond typical commercial software profilers, because S-Check allows software engineers to determine effects of changes in their codes without them having to make actual changes and rerunning programs. Existing commercial tools only show the time required to execute particular parts of the code, but do not determine whether changes to slow parts of the program will significantly improve performance. With parallel programs, it is quite possible for lightly used sections still to be bottlenecks. Such sections are hard to spot without intimate (and expensive) knowledge of the specimen code and host system. Addressing this problem, S-Check automatically assesses points in the code where changes could be significant. For a detailed view of S-Check, you can access a description of this product at http://www.scheck.nist.gov/scheck.

Advanced Information Processing, Recognition and Storage Systems

In collaboration with the Information Access and User Interfaces Division and the Mathematical and Computational Sciences Division, we built two hybrid optical (combining optical processing and digital neural networks) information systems: a three-dimensional volume holographic storage system and an optical pattern recognition system. Our emphasis in this project is to improve the metrology, accuracy, reliability, and reproducibility of these photonic systems by combining digital and neural network approaches. The initial phase of work was supported by the Federal Bureau of Investigation (FBI).

The systems were tested for processing mugshot images and fingerprints with an almost 100 percent recognition rate for correct inputs without distortion. Also, a digital method to improve the holographic image quality has been experimentally tested with great success. The systems were demonstrated to the FBI, the Central Intelligence Agency, the University of Arizona, and Carnegie Mellon University. These systems are expected to play important roles in handling large amounts of data at a very fast rate.

Volume holographic storage has a great potential storage capacity of the equivalent of a 100-1000 CD's in a one cubic centimeter crystal with an access time of near one million pages per second. As part of our initial research, we built a working holographic memory system fully interfaced with a computer. The system was tested using FBI mugshots and fingerprint images. It provided a reasonable amount of image quality (dynamic range, resolution, etc.) to suit FBI requirements.

An investigation into improving the quality of a holographic image by removing speckle noise was successfully implemented and tested. A series of experiments and analyses to support the idea and to prove its validity have been performed. Various noise sources have been identified and related measurement issues have been raised. Our work complements the Defense Advanced Research Projects Agency's holographic storage project by emphasizing the metrology of holographic storage. Potential customers for storage devices with large capacity and fast access, such as video-on-demand, include the FBI, NIST, the National Security Agency, and the data storage industry.

Automatic pattern recognition is important in a variety of information applications, such as automatic information handling, processing, and security. We constructed a real-time hybrid optical pattern recognition system that can be used for various pattern recognition, identification, and classification schemes. The system uses both optical pattern recognition and digital neural networks to monitor each stage of information processing such as input images loaded on an SLM (spatial light modulator), two-dimensional Fourier spectra, and correlation outputs. The system was tested for characters, FBI mugshot images, and real-time fingerprints (through a real-time fingerprint scanner) with a high recognition rate (almost 100 percent recognition rate for correct inputs).

Distortion-invariant recognition by optimizing filters using neural network algorithms, remains to be improved. A holographic recording process can accommodate distortional variations to allow a reasonable amount of distortion-invariant fingerprint recognition. Our system will use various hybrid approaches and become a testbed for commercial hybrid optical verification systems. The market is increasing for network access security applications, such as the Internet combined with real-time fingerprint matching for user verification. Areas of use include verification of financial instruments (credit and debit cards), access to proprietary databases, or exit/entry verification.

In the area of storage media, we developed techniques for measuring the monitoring and reporting of media errors on optical disks. Optical disk drives are designed with powerful, but not unlimited, error correction capabilities. If the level of media error exceeds the error detection and correction mechanisms implemented in the device controller, the data cannot be corrected by the device and data loss might occur. Our work led to a voluntary industry standard specifying techniques that can be used both initially when the data is transferred to the media and periodically to monitor the status of that data. A drive that implements these techniques can provide users and systems integrators with early warning mechanisms that decrease the possibility of data loss.

Investigations on optical disk data integrity included comprehensive research on the care and handling properties of all types of optical disks including Write-Once Read Many Times (WORM) media, re-writable media, CD-ROMs and CD-R media. An extensive set of experiments on hundreds of optical disks aimed at determining which environments, substances, and fields could be harmful or potentially harmful to the disks. The experiments included smoke from different materials, fire extinguishers, food substances, different temperature and humidity environments, cleaning agents including water, surfactants and alcohol, paints and wax fumes, pressure tests, magnetic fields, electrostatic discharges, X-rays and gamma-rays, read/write/erase cycles, gasoline, diesel and brake fluids. Although some of the disks were affected by some of the experiments, in general optical disks have demonstrated a high resilience to many different environments and care and handling conditions.

Advancing the NIST Scientific Computing Environment

Two major upgrades in the Central Computing Facility expanded the capabilities of NIST scientific computing and give improved service to our customers. A Cray C96 with 2 Gigabytes of memory replaced the over-committed Cray Y/MP 4. This upgrade permitted increased throughput focusing on high performance batch computing.

The continued upgrading of the IBM SP2 expanded the capabilities previously provided for scalable parallel processing. The SP2 has grown to 31 nodes; 30 of the nodes have 512MB of memory with 2.4 GB of temporary disk storage, providing a configurable environment for production and research parallel projects.

State-of-the-Art Networking and Telecommunications

The Network and Telecommunications Systems Group initiated a network upgrade project to enhance the existing PEPnet/Eznet network infrastructure, which supports up to 10 Megabits of data per second (Mbps), with Category-5 (CAT5) connections, which can support up to 155 Mbps. The existing network is implemented over the telephone system wiring. So far, the NIST buildings wired with CAT5 are NIST North (Building 820) and the Technology Building (Building 225), while plans are being finalized for the new Advanced Chemical Sciences Laboratory building which is currently being built. More campus sites will be added as network congestion becomes apparent.

The CAT5 segments of the networks will be dedicated to computers requiring large bandwidths, primarily servers, while average users on the existing segments will benefit from increased segmentation of the networks and the placement of network switches that enable proactive network management. This combination of state-of-the-art networking technology with the large network installation base will provide NIST's PEPnet and EZnet users with reliable network service for the foreseeable future while protecting NIST's investment in the existing infrastructure. One exciting and ongoing project is the connection of the NIST network through its ATM switches, allowing NIST to robustly connect to the national ATM network. The Division is also in the process of installing a computer testbed linked to an ATM switch, as well as testing the effectiveness of fiber-to-the-desktop (FTTD) for advanced workstation environments.

DISTRIBUTED COMPUTING AND INFORMATION SERVICES DIVISION

Chief: **Oscar Farah**

Group Managers: **Bob Crosson, Distributed Processing and Operating Systems Support**
Mark Williamson, Information Processing Support
Robert Lee, Administrative Computing Support
Oscar Farah (Acting), PC Support

Distributed Processing and Operating Systems Support

In the past year, the Distributed Processing and Operating Systems Support Group had a number of significant accomplishments. The major project was the installation of the Sun Microsystems SparcServer 1000E as the replacement for the MICF for electronic mail users. Hundreds of user accounts were moved off the MICF to the Sun for e-mail service. This machine now processes over 3,000 e-mail messages per day.

A second significant project accomplished by the Group was installing the Synchronize calendaring application for use by all NIST staff. We initially used a small IBM RS6000 as a server for the operational demonstration. The package was then moved to one processor of a large RS6000 dual-processor machine and subsequently to the Sun Microsystems SparcServer 1000E. As this reconfiguration took place, the number of user accounts grew from less that 300 to more that 800. We continued to provide uninterrupted service to all users during the server replacement activity.

Another Group accomplishment was the upgrading of two more file servers from the SunOS operating system to the Solaris operating system. The goal was to have all servers running Solaris, but, as was experienced by migrating the first two servers, many problems must be resolved before the migration will be complete.

The Group also acquired a Digital Equipment Corporation Alpha 1000/266 server running Microsoft Windows NT version 3.51. The operating system was recently upgraded to Windows NT version 4.0. This machine is being used to determine the viability and limitations of Windows NT and whether it is advisable to install such servers at NIST to provide file and printer-sharing services.

Finally, members of the Group designed a new NIST Training Room and installed 21 PCs. The project included having the office space modified, installing a raised floor and special lighting, and equipping the room with the necessary PCs, printers, and projectors.

Information Processing Support

In FY 1996, ITL established a new Information Processing Support Group. The mission of the Group is to design, implement, and maintain NIST's automated information processing systems. This includes the design, implementation, and maintenance of NIST's World Wide Web (WWW), electronic commerce, and information delivery systems. The Group also provides consulting and training on information delivery services and on designing, implementing, and supporting the paperless office of the future.

Staff members developed and implemented an enterprise-wide WWW hosting facility for use by the NIST Operating Units (OUs) with an architecture that includes external and internal Web servers. The external servers, http://www.nist.gov in Gaithersburg, Maryland, and http://www.boulder.nist.gov in Boulder, Colorado, are accessible to all Internet users and present NIST public information. The internal server, http://www-i.nist.gov, is used exclusively for the NIST intranet publishing of information for the use of NIST staff only. The internal server serves both Gaithersburg and Boulder.

The Group uses the Network File System (NFS) protocol to create virtual drives on the OU's PCs or workstations. These virtual drives, which are physically located on the Web servers, are used by the OUs to store the information they would like to publish. The Web servers use the most up-to-date software, are secured against tampering, and are centrally monitored and maintained 24 hours a day, 7 days a week. Thus, the OUs are not required to use valuable resources to acquire and maintain their own servers and their ability to publish and maintain their own information is not affected.

Additionally, we incorporated other servers for anonymous File Transport Protocol (FTP), for the NIST Locator, and for operation of an automated Travel Manager. Staff members also provided assistance with home page development, WWW CGI programs, online forms, multimedia presentations, and office automated information systems. In FY 1996, we developed new WWW sites for the Office of Quality Programs, http://www.quality.nist.gov; the Information Technology Laboratory, http://www.itl.nist.gov; and a WWW site and information management system for the Advanced Chemical Sciences construction project, http://www.nist.gov/acsl. We also provided WWW programming support to the Manufacturing Extension Partnership in the customizing of WWW search engines and in developing a WWW-based calendaring system.

Administrative Computing Support

In FY 1996, the Administrative Computing Support Group worked on the Commerce Administrative Management System (CAMS) in addition to its usual support and programming for the administrative functional areas and the implementation of new administrative information databases. The staff also attended seminars, presentations, and meetings to learn and discuss the impact of the Year 2000 issue.

The CAMS effort, at times, took a considerable amount of staff resources. We participate in committees on several of the CAMS modules including the Core Financial System (CFS), the Personal Property Module, the Small Purchase System, and the Receiving System. Staff members attend meetings, prepare documentation, convert data, supply test data, work on interface programs, test the system, and assist staff at the CAMS Implementation Center. Additionally, staff attend Oracle Classes to learn and use the tools provided in order to support the CAMS system when implemented. Some of the staff are already involved with the Database Administration activities supporting this system such as establishing databases for user identification, database roles, and tracking users privileges. Other activities include installing SQLNET, TCPIP adaptors, FORMS 4.5 software and runtime modules, printers and printer configurations, and the Oracle Web Service; establishing and maintaining backup and recovery for the UNIX servers, and adding new users, and starting/shutting down databases.

Some of the highlights for the general administrative functional areas included the conversion of most of the financial reports from the COBOL and UNISYS platform to the Financial Databases and the IBM/VM (MICF) platform; the conversion of the FY 1993 financial database from the UNISYS to the MICF platform; and development of the Treasury Payment database for the Office of the Comptroller. We also implemented a new Report Subscription service to facilitate the electronic dissemination of financial reports. Time was spent in the validation and verification of the Time and Attendance data as processed by the National Finance Center (NFC) and catching up with normal business processing that was disrupted in early 1996.

We implemented many new upgrades to administrative support software; these included a new release of the Automated Classification System, the Payout System, the Plant System, the Travel Database system, and the Quick Procurement System. The Procurement Lookup was converted from the UNISYS to the MICF to facilitate obtaining procurement status information. The new applications released into production included the Reorganization System, the Student Employment Program Applicant System, and Procurement Integrity Information System.

SOFTWARE DIAGNOSTICS AND CONFORMANCE TESTING DIVISION

Chief: **Mark W. Skall**
Group Managers: **D. Richard Kuhn, Software Quality**
Lynne S. Rosenthal, Conformance Testing
Bruce K. Rosen, Software Standards

Activities in the Software Diagnostics and Conformance Testing Division focus on the development of software evaluation technology, conformance tests, and standards that can be used to assist U.S. industry in the development of high-quality software. In this role, the Division develops software testing tools and methods, participates with industry in the development of forward-looking information technology standards, and leads efforts for the development of conformance tests even at the early development stage of standards.

Software Analysis Tools

Division researchers participate in the development of tools for static and dynamic analysis of software, focused on measuring conformance to specifications and diagnosis of the causes for deviations from specifications. Included is work on static analysis tools for program slicing and generation of paths for basis testing, and the extension of object-oriented languages to allow for the detection of pre- and post-condition violations.

For the Nuclear Regulatory Commission, ITL developed the Unravel Program Slicer which computes "slices" of C programs, where a slice is a subset of the program that contains all lines of code that can directly or indirectly affect the value of a particular variable at a particular point. The tool assists in the effort to debug or test a program since it allows the programmer to focus on those parts of the program that are relevant to the logic in question. Other front ends for the Unravel Program Slicer are being considered for development for other programming languages such as C++ or JAVA.

We are developing a second tool for program maintenance and modification, based on the Unravel tool. This tool, called Surgeon's Assistant, is one that would make it possible to isolate program components for modification and adaptation, make the desired modifications to those isolated program components, and assess the impact of those modifications. The tool may also be an important aid in the development of reuse libraries and in reverse engineering of legacy systems.

In the area of object-oriented programming languages, we initiated a project to extend those languages to include program correctness statements. These statements would be used by programmers to assert conditions which should be met at a given point in the program, thus improving program quality by providing for the immediate notification and location of program behavior. The result of this project is a tool that adds source code instrumentation to detect pre- or post-condition violations, trace values, or diagnose error conditions.

To assist industry in the evaluation of the methods and tools they use to improve software quality, we are developing a library of standard reference materials consisting of software with known errors. This library can be used by software developers to determine the effectiveness of the test tools and techniques they use in developing their systems. As part of this effort, we plan to develop statistical methods of evaluating testing procedures and software development tools and techniques.

Software Conformance Testing

Division researchers develop tests which determine whether implementations of public specifications conform to that specification. We seek to work closely with outside organizations to establish, under the purview of those outside organizations, certification test services for the issuing of certificates of conformance.

In cooperation with the Air Transport Association (ATA), ITL is building Computer Graphics Metafile (CGM) conformance test suites and is developing a certification test service. Also cooperating in this effort is the Aerospace Industries Association (AIA). Work is under way to develop test suites and automated testing tools for a different CGM profile to be used in expanding the test suite coverage of the ATA profile.

ITL is now completing its work to develop conformance tests for features standardized by the Intermediate SQL level standard for Database Language SQL. With the completion of these final test suites, SQL implementers will have available an authoritative set of tests to be applied during the early stages of product development when it is easiest to correct any errors that are discovered.

In cooperation with the Department of Defense, we are completing the development of the Ada compiler validation capability and the associated conformance testing program procedures. The NIST Ada95 validation program will provide a common economical measure which should substantially increase the reliability of safety critical and non-safety critical Ada tools and products.

A new area of conformance test development is the work now ongoing to develop a test suite in the area of Virtual Reality Modeling Language (VRML). VRML is quickly being integrated into multiple tools that are being used on the Internet for the viewing of 3-D objects. It is important to establish a VRML test suite that tests for complete conformance to all portions of the VRML specifications. To develop these test suites, ITL researchers are examining the VRML specifications and working with companies and individuals that have created some existing test files, in order to determine how to best achieve full and complete test suite coverage of the VMRL specification.

As a research project, we are investigating new and more efficient approaches to the development of conformance tests. Current conformance tests are developed through the extremely time-consuming process of developing falsification tests. Such testing, while extremely useful, can never cover all requirements and cannot provide total proof of correctness. We are looking at alternatives to falsification testing such as proofs of correctness and statistical measures of correctness. In addition, we are investigating the effectiveness of using automated test generation methods to develop conformance tests for specifications of standards. This research could lead to faster ways of developing conformance tests, resulting in an increased capability for product developers to determine if their products work according to specifications.

Forward-Looking Standards

ITL researchers seek to make significant technical contributions to standards which are on the cutting edge of software technology. In this effort, we pursue work in areas that have a research component and for which vendors do not yet have implementations or other vested interests in the work.

In the area of Role Based Access Control (RBAC) on the World Wide Web, ITL researchers are developing a technical specification, including a formal description, of RBAC on the Web. We are also developing a proof-of-concept model of such a product, and an abstract and physical test suite to measure conformance to the RBAC model.

Users of standards are often faced with the daunting task of trying to locate and access standards that are appropriate to their work. To simplify this task, we are developing a taxonomy and framework for standards that can be used to both coordinate the development of forward-looking standards and to assist potential users of standards in finding and applying those standards that are applicable to their particular requirements. As part of this effort, an online standards locating and retrieval capability, offering the user multiple interfaces, will be implemented to provide access to standards from both government and commercial sources.

To improve the standards development process, ITL is investigating the development of a method that would enable standards developers to formally define those parts of their specification that are intended to interface with other standards, so that an automated mechanism could be developed that would allow for testing of two or more specifications to ensure that there is no conflict between the specifications. This would make it possible to specify the common parts of interacting standards in a manner that would allow it to be precisely determined if those standards are compatible. This work would make it easier to develop software, based on those standards, that would integrate correctly since it would have already been verified that the interface specifications of those underlying standards were done in a manner that makes them compatible.

In cooperation with the Environmental Protection Agency, NIST initiated a project to focus on development of several specific infrastructure components needed for the intelligent integration of database information with intelligent information services techniques. Particular attention is being paid to the application of classification taxonomies and ontologies, as related to development of an Environmental Data Registry, in order to provide for testable, high-quality access interfaces for multiple types of software that serve as information search engines. As part of this task, we are investigating the application of specified infrastructure components to the research area of network Object Registration.

STATISTICAL ENGINEERING DIVISION

Chief: **Lynne Hare**
Group Managers: **M. Carroll Croarkin, Measurement Process Evaluation**
Keith Eberhardt, Statistical Modeling and Analysis

The Statistical Engineering Division seeks to catalyze scientific and industrial research through the application of statistical methods to the experimentation and data analysis underlying the empirical information gathering processes critical to NIST scientists and engineers. To accomplish this mission, the Division develops strong collaborative research relationships with NIST staff in all fields, maintains expertise in the development of statistical methods relevant to measurement science and technology, and ensures that NIST staff have access to information on the latest statistical modeling and analysis techniques necessary for their research.

Statistical Consulting

The Division collaborates with NIST staff on research projects where optimal experiment design, statistical modeling, and data analysis can play a significant role in improving measurement processes and gaining scientific insight. Staff members also provide general statistical consulting services to NIST scientists working in all aspects of NIST's mission. Specific contributions include:

- Leadership in the establishment of a high standard of statistical practice within NIST via interactions with technical staff, publications, workshops, and seminars;
- Design and analysis of experiments, and evaluation of measurement uncertainties for the NIST Standard Reference Materials (SRM) and Calibration Programs;
- Design and analysis of experiments, and evaluation of protocols and processes associated with NIST scientific endeavors;
- Support of NIST industrial clients engaged in the design and analysis of experiments;
- Development of statistical and probabilistic models for physical science and engineering applications;
- Development of statistical methodology to enhance collaborative research with other NIST laboratories;
- Advancement of statistical methodology via development of algorithms and software; and
- Transfer of statistically based measurement methodology to industry through direct interactions with industrial clients, publications, workshops, and seminars.

The following examples of statistical applications are typical of the work of this Division.

Environmental Radioactivity Standard Reference Material (SRM) and Radionuclide Speciation

In today's pollution-sensitive world, it has become increasingly more important to have available well-characterized SRMs of a natural "matrix" type which may be used in laboratory tests of measurements of environmental radioactivity. Such materials would be used in the evaluation of competing analytical methods, and also in the cross-comparison of interlaboratory data, at both the national and international levels.

Division statisticians collaborated with scientists in NIST's Physics Laboratory who constructed an SRM consisting of a 12-component natural matrix ocean specimen. The 1000-bottle SRM 4357 has two sediment sources: the Chesapeake Bay (benign) and the Irish Sea ("hot"). The goal of the project was to determine global (valid across all 1000 bottles) values and uncertainties for each of the 12 elements (radionuclides): potassium, radium, thorium, strontium, uranium, etc. The certification required three steps, all with technical challenges. An interesting distributional conclusion was that the eight "natural" radionuclides tended to have a normal distribution, while the last four "man-made" radionuclides tended to have a Weibull distribution.

Computational Metrology of Manufactured Parts

U.S. industry uses more than 20,000 coordinate measurement machines (CMMs). A CMM helps determine if a part conforms to design specifications by measuring the coordinates of a sample of locations on the part surface. Currently, there is no rigorous methodology to determine the accuracy and the precision of the measurements from a CMM. Consequently, CMMs are considered uncalibrated and not traceable to the International Standard (SI) according to International Organization for Standardization (ISO) definitions. Developing calibration methodology for CMMs is necessary for U.S. companies to trade internationally. Additionally, the methodology would promote improvement in quality and efficiency through better determination of part dimensions.

As part of a NIST competency project, Division scientists play an active role in the cross-disciplinary group that is making significant progress towards solving this problem. Initially, the group concentrated on understanding and modeling the CMM probe, which is the largest source of error in the measuring process. The probe is the component of the CMM that senses the contact with the part being measured. The most common class of probes has a construction that leads to pronounced systematic effect in the CMM measurements. Through a large modeling effort, the group produced a reliable model that allows for real-time correction of measurements. The result is an improved measurement system without significant added costs. We also developed an uncertainty procedure for use with the model, a procedure which addresses the overall project goal of traceability.

Statistical Analysis of Retardance Measurements

Optical communication, data storage, ellipsometry, sensor and other optoelectronic systems often use linear retarders to control or analyze optical signals. Often these systems require retarders with specific and/or accurately known values of retardance. Division scientists collaborated with NIST's Electronics and Electrical Engineering Laboratory to develop a quarterwave linear retarder designed to have a retardance stable within 0.1° over a variety of operational and environmental conditions. Three methods are used to measure retardance. One method uses a modified version of standard polarimetric measurements and uses rotating polarizers. Linearly polarized light, with known orientation, is incident on the retarder and the light emerges with an elliptical polarization. The intensities of the perpendicular and parallel states of the emerging light are measured. Many (112) experiments were run to determine the retardance of five rhombs. One finding of the project suggests that the goal of retardance measurement with uncertainty less than 0.1° is reachable with this system.

Measurement Control for Heart Valve Manufacturer

During the process of manufacturing artificial heart valves, Medical Carbon Research, Inc. (MCRI), makes a very large number of measurements using a coordinate measurement machine (CMM). The company contacted our Division and NIST's Manufacturing Engineering Laboratory because they were experiencing difficulty in establishing control charts to monitor all 146 dimensions of their multivariate measurements on a check standard artifact. In particular, there were too many out-of-control signals being generated when they used 146 univariate control charts and required that all dimensions be inside the control limits for each complete set of measurements.

To address the practical problem, we transformed the raw data matrix, consisting of 24 replications of a 146-dimensional vector, into principal components. Analysis showed the expected result that a very large proportion of the variation is captured in the first one to three principal components. We transmitted this result to the company, along with a copy of Dataplot software and an example program to compute the principal components and construct a control chart for them. MCRI subsequently installed Dataplot and successfully reproduced the calculation of the principal components and the control chart.

NIST Ceramic Machining Consortium

In 1992, NIST established a consortium with members from industry, academia, and government to assist U.S. industry in the development of precision machining for the manufacturing of cost-effective advanced ceramic products. In collaboration with the Materials Science and Engineering Laboratory, the Statistical Engineering Division plays a critical role in this effort. The goal of the consortium is to collect and analyze data on the effect of grinding parameters on ceramic properties and performance. The resulting Ceramic Machinability Database provides access to data for different types of ceramics and helps users develop machining plans for the cost-effective production of ceramic parts.

Our expertise focused on the silicon nitride project, where conclusions regarding important grinding parameters could potentially be contaminated by other factors such as laboratory, batch, etc. We contributed a careful design for this large-scale multi-laboratory experiment to assure the validity of the conclusions. Our statisticians further provided the data analysis expertise in ascertaining important grinding factors, uncovering significant non-grinding factors, identifying interactions, and establishing optimal settings.

Statistical Reference Data Sets

Working jointly with colleagues in the Mathematical and Computational Sciences Division, we have constructed a large suite of statistical reference data sets for use by users and writers of statistical software to test the accuracy of statistical analyses. Data sets are in downloadable form for ease of use. Solutions to commonly used summary statistics are provided. Users may select data sets in four categories: univariate statistics, multiple regression, non-linear regression, and analysis of variance. This selection will be augmented with at least three more categories.

Information
Technology
Laboratory

Interactions and Accomplishments

Selected Staff Accomplishments

Department of Commerce Medal Awards and NIST Awards

John K. Antonishek received a 1996 Bronze Medal for the installation, implementation, and management of the NIST North network and telephone systems. He also received the 1996 NIST Safety Award for Superior Accomplishment for his safety leadership in the installation of the computer communication network at the NIST North campus.

Patricia D. Barnett received a 1996 Bronze Medal for extraordinary service in supporting the hardware and software for the NIST-wide e-mail and calendaring functions.

Lisa Carnahan received a 1995 Bronze Medal for establishing the FIPS 140-1 validation program whereby accredited laboratories test cryptographic products for conformance to NIST standards.

Christopher Dabrowski received a 1995 Bronze Medal for technical enhancement of domain analysis and its application to the development of an architecture for the National Information Infrastructure.

Judith E. Devaney, Robert R. Lipman, and William F. Mitchell received a 1996 Bronze Medal Group Award for creation of the NIST Parallel Applications Development Environment (PADE).

Cita M. Furlani received a 1995 Silver Medal for the leadership of interagency activities that advance applications of information technology on the National Information Infrastructure.

Barbara Guttman and **Edward Roback** jointly received a 1995 Bronze Medal for developing *An Introduction to Computer Security: The NIST Handbook* which promotes comprehensive, cost-effective security programs in the private and public arenas.

Shirley Hurwitz received a 1995 Bronze Medal for leadership of NIST/industry programs in database interoperability and the application of distributed database technologies to electronic commerce.

Stefan D. Leigh received a 1995 Bronze Medal for extraordinary success and dedication in enhancing the effectiveness of statistical collaborations at NIST.

Walter S. Liggett, Jr. shared the 1996 Edward Bennett Rosa Award with four other NIST scientists for the development and international acceptance of a method for the more accurate determination of Rockwell C Hardness, a measured material property of great importance in manufacturing and commerce.

James R. Lyle received a 1996 Bronze Medal for advancing the state of the art and practice in static analysis methods for computer software.

David S. Pallett received a 1996 Bronze Medal for leadership in the development of speech corpora and the use of these corpora by spoken language researchers.

Marianne Swanson and John P. Wack received a 1996 Bronze Medal Group Award for the successful establishment and management of the Forum of Incident Response and Security Teams (FIRST).

External Recognition

Thomas C. Bagg posthumously received the Thomas C. Bagg Lifetime Achievement Award established in his honor for his significant contribution to the AIIM Standards Program. A NIST employee since 1941, Bagg conducted original research in physics, imaging science, computer systems, document management, micrographics, information retrieval, and electrical engineering for 50 years until his death in 1995.

Isabel Beichl became a columnist for the IEEE journal *Computing Science and Engineering*, coauthoring a monthly article on "Computing Prescriptions."

Daniel R. Benigni was elected Vice President for Professional Activities and Chairman of the United States Activities Board (IEEE-USA) for 1997. IEEE-USA promotes the career and public policy interests of the more than 230,000 IEEE members in the United States.

Paul Boggs serves on the Editorial Board of the *SIAM Journal of Optimization*, the *Applied Mathematics Letters* and the *SIAM News*. He was also appointed to the SIAM Science Policy Committee and serves on the review panel for the Army Research Office and the Center for Computing Science.

Ronald Boisvert was appointed to the ACM Publications Board and reappointed as Editor-in-Chief for the *ACM Transactions on Mathematical Software* for a second three-year term. He was also elected a full member of the International Federation for Information Processing (IFIP) Working Group 2.5 (Numerical Software).

Leslie Collica received the ATM Forum Spotlight Award for her technical contributions and her work as Editor and Vice-Chair of the Testing Working Group at the December 1996 ATM Forum.

David Cypher received from the ATM Forum the Editorship of the Protocol Implementation Conformance Statement (PICS) of the Private Network to Network Interface (PNNI) standard.

Keith Eberhardt was elected Fellow of the American Statistical Association.

Michael Garris received the Award for Excellence in Technology Transfer 1996 from the Federal Laboratory Consortium. His software distribution technology is a form-based handprint system for evaluating optical character recognition (OCR). Garris and his associates transferred this state-of-the-art technology in the public domain to numerous industry and government users via a CD-ROM using ISO-9660 format.

John Hagedorn received a Finalist award in the Telly Award competition, an international competition honoring non-network television commercials and programs, and non-broadcast video & film productions, for his computer graphics contribution to the video "Building Fire Research Laboratory - Your Partner in Building."

Lynne B. Hare is the Chair, Section on Quality and Productivity, American Statistical Association for 1996 and the Awards Committee Chair, Statistics Division, American Society for Quality Control, 1995-96. He also serves on the Management Committee of *Technometrics*.

Raghu Kacker was elected Ordinary Member of the International Statistics Institute.

Samuel J. Lomonaco serves as Associate Editor of the *Journal of Knot Theory and its Ramifications.*

Daniel Lozier was appointed as Associate Editor of *Mathematics of Computation* and serves as an Editor of the *NIST Journal of Research.*

Roger J. Martin received the 1995 Hans Karlsson Award from the IEEE Computer Society for leadership in the timely completion of test methods which assure quality and dependability for the standards customer, completeness for the portable application builder, and consensus of the whole community.

Victor McCrary was invited by the prestigious Sigma Xi Distinguished Lectureships Program to serve on the 60th College of Distinguished Lecturers for a two-year term from July 1997 to June 1999.

Geoffrey B. McFadden is on the Editorial Board of the *SIAM Journal of Applied Mathematics* and the *Journal of Computational Physics.*

William F. Mitchell developed the MGGHAT package for adaptive solution of partial differential equations which was selected as a finalist for SIAM's 1995 Wilkinson Prize for Numerical Software.

Fernando L. Podio received the 1996 Standards Excellence Award from the Association for Information and Image Management International (AIIM) for outstanding and valuable contributions to industry through his efforts in the AIIM standards program, especially in standards development in the area of mass storage systems, particularly optical disk.

Roldan Pozo received a 1996 Presidential Early Career Award for Scientists and Engineers, the highest honor bestowed by the U.S. government for outstanding scientists and engineers beginning their independent research careers. The award recognizes exceptional potential for leadership at the frontiers of scientific knowledge during the twenty-first century.

John Roberts was awarded the Video Electronics Standards Association (VESA) Crystal Globe Award. The award was given for service to the Flat Panel Display Interface Committee and the Monitor Committee, including service as Secretary, and for helping VESA to establish its technical electronic mailing lists and file-transfer-protocol site.

Marianne Swanson received the 1996 Leadership and Achievement Award from the Industry Advisory Council of the Federation of Government Information Processing Councils for her work with the Government Information Technology Services (GITS) Board in promoting support mechanisms for governmentwide security initiatives.

C.M. Wang served as President of the American Statistical Association, Colorado-Wyoming Chapter, 1995-96.

PARTICIPATION IN VOLUNTARY STANDARDS ACTIVITIES

TECHNICAL ACTIVITIES

■ Accredited Standards Committee (ASC)

Technical Committee X3, Information Technology

X3H2 (JTC1/SC21/WG3) Database	Elizabeth Fong
X3H3 (JTC1/SC24) Computer Graphics & Image Processing - Virtual Reality Modeling Language (VRML) Reference Implementation and Conformance Tests	Mark Skall, Mary Brady, and Lynne Rosenthal
X3H3.3 (IEC/JTC1/SC24/WG6) Multimedia Presentation and Interchange	Lynne Rosenthal and Mary Brady
X3H3.8 (JTC1/SC24/WG7) Image Processing & Interchange	Mark Skall and Susan Sherrick
X3H7 Object Information Management	Elizabeth Fong
X3L1 (ISO TC 211) Geographic Information Systems	Christopher Dabrowski
X3L3.2 (JTC1/SC29/WG10) Still Image Coding	Robert McCabe
X3L8 (JTC1/SC14) Data Representation	Judith Newton and Bruce Rosen
X3L8.6 (JTC1/SC14/WG4) Classification of Data Elements	Judith Newton
X3T4 (JTC1/SC27) IT Security Techniques	Eugene Troy and Ellen Flahavin

Technical Committee X9, Financial Services

X9F Data and Financial Information Security	Miles Smid
X9F.1 Public Key Cryptography for Financial Systems	Miles Smid
X9F.3 Wholesale Bank Security	Elaine Barker
X9F.4 Authentication and Access Control	James Dray

U.S. Technical Advisory Group (TAG) to JTC1/SC22 Programming Languages, Their Environments and Systems Software Interfaces - Java Study Group	Gary Fisher

■ Association for Computing Machinery (ACM)	
Role Based Access Control	John Barkley
■ Association for Information and Image Management (AIIM)	
Committee C21 Storage Devices and Applications	Fernando Podio
■ American National Standards Institute (ANSI)/National Information Standards Organization (NISO)	
ANSI/NISO Z39.50 Implementors' Group - ZPRISE Prototype	Paul Over
■ American Society for Testing and Materials (ASTM)	
E-11 Quality and Statistics	Carroll Croarkin
■ Asynchronous Transfer Mode (ATM) Forum	
Private Network to Network Interface Group	David Cypher
Testing Working Group	Leslie Collica
Traffic Management, Residential Broadband, Service Applications	David Su
■ Digital Audio Visual Council (DAVIC)	Karen Hsing
■ European Workshop Manufacturers Association (ECMA)	
Java Scripting Language Study Group	Gary Fisher
■ Institute of Electrical and Electronics Engineers (IEEE)	
P802.14 Cable Modems	David Su
■ Internet Engineering Task Force (IETF)	
INT Internet Area (IPv6, IP/ATM)	Robert Glenn, Douglas Montgomery, and Hsin Fang
MGMT Management Area (SNMP, MIBs)	Wo Chang
RTG Routing Area	Douglas Montgomery
SEC Security Protocols Area	Robert Glenn and Shu-Jen Chang
TSV Transport Area (RSVP, RTP)	Douglas Montgomery and Shu-Jen Chang
Privacy & Security Research Group	James Dray and Donna Dodson
■ Interactive Multimedia Association (IMA)	
Metadata Standard for Digital Objects	Tom Rhodes

- **International Multimedia Teleconferencing Consortium (IMTC)**

Video Conferencing Standards (H.324/H.323/H.320/T.120)	Jean-Philippe Favreau

- **IGES/PDES Organization (IPO)** of the U.S. Product Data Association

(ISO TC 184/SC4)	Lynne Rosenthal

- **Object Management Group (OMG)**

Applications Development Working Group	Barbara Cuthill and Tom Rhodes
Business Object Management	Elizabeth Fong
Common Facilities Task Force	Barbara Cuthill
Object Request Broker Task Force	John Barkley
Object Services Task Force	John Barkley and Tom Rhodes
Portable Common Tool Environment (PCTE) Special Interest Group	Barbara Cuthill and Tom Rhodes
User SIG - Metrics WG	John Barkley

- **Open Group** (formerly X/Open)

Security Group	Shu-Jen Chang

- **T1S1**

Services, Architectures and Signalling	David Cypher

- **Video Electronics Standards Association (VESA)**

Flat Panel Display Interface Committee	John Roberts

- **Virtual Reality Modeling Language (VRML) Consortium**

VRML	Lynne Rosenthal

MANAGEMENT ACTIVITIES

ASC X3 Information Technology	Michael Hogan
ASC X3/OMC Operational Management Committee	Michael Hogan and Robert Rountree
ASC X3/PPC Policy and Procedures Committee	Michael Hogan
ASC X9 Financial Services	Miles Smid and Donna Dodson
ASC X12 Electronic Data Interchange	Jean-Philippe Favreau
AIIM Standards Board	Fernando Podio
ANSI Executive Standards Council	Michael Hogan
ANSI Healthcare Informatics Standards Board (HISB)	Susan Katz

MANAGEMENT ACTIVITIES (continued)

ANSI Information Infrastructure Standards Panel (IISP) - Framework for Standards	Michael Hogan, Christopher Dabrowski, etc.
ANSI Information Infrastructure Standards Panel (IISP) Steering Committee	Shukri Wakid
ANSI Information Systems Standards Board (ISSB)	Michael Hogan
ATM Forum	David Su
Cross Industry Working Team (XIWT)	Shukri Wakid and Jerry Linn
IEEE Standards Board	Robert Rountree
JTC1 TAG (U.S. TAG to ISO/IEC JTC1 on Information Technology) and JTC1	Michael Hogan
Network Management Forum	Frances Nielsen
North American Interoperability Policy Council (IPC)	Michael Hogan
North American ISDN Users' Forum (NIUF)	Leslie Collica
Object Management Group (OMG)	John Barkley
U.S. TAG for ISO TC 69 Applications of Statistical Methods	Carroll Croarkin and Raghu Kacker
Video Electronics Standards Association (VESA)	John Roberts

Industry Interactions

ITL participates in many consortia and industry interest groups including the following:

Air Transport Association (ATA) and Aerospace Industries Association (AIA)

The ATA and AIA are international nonprofit organizations for the airline industry and aerospace suppliers. The ATA and AIA consist of the major airline companies, aerospace industries, and software and systems suppliers of the commercial aerospace industry. The ATA, AIA, and ITL are working together to develop a graphics profile and conformance tests methods for the interchange of graphics data within the commercial aerospace industry. The commercial aircraft industry is moving away from paper-based delivery of maintenance data to digital delivery. Conformance testing is critical in ensuring that graphics tools and implementations conform to the ATA profile and ease the transition to digital delivery of data. Lynne Rosenthal is the ITL contact.

Association for Information and Image Management International (AIIM)

ITL participates in AIIM International, the world's leading association for information industry users and providers. Members include key U.S. players of the information, document, and image management industry. AIIM is an accredited American National Standards Institute (ANSI) standards development organization involved in creating, disseminating, and promoting industry standards worldwide. Fernando Podio works with the Optical Tape Study Group and participates in the File-Level Metadata for Portability of Sequential Storage Media Study Group.

Asynchronous Transfer Mode (ATM) Forum

The ATM Forum is an international nonprofit organization which accelerates the use of ATM products and services through a rapid convergence of interoperability specifications. About 170 U.S. telecommunications corporations comprise the ATM Forum membership. Through the forum, ITL works with Bellcore, test equipment vendors such as Tekelec and Hewlett-Packard, and ATM switch vendors to develop interoperability test specifications and conformance test suites. We also participate in the Signalling and Traffic Management Working Group to develop ATM service protocols. David Su is the ITL principal.

Cross Industry Working Team (XIWT)

The Cross Industry Working Team (XIWT) is a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful, sustainable national information infrastructure (NII). Members include firms from the computer, networking, telecommunications, publishing and banking sectors, and others with business interests in the NII. NIST is represented on the executive committee by R.J. (Jerry) Linn; other ITL representatives participate in working groups related to their research and development activities.

Digital Audio Visual Council (DAVIC)

The Digital Audio Visual Council (DAVIC) is an international consortium for the emerging digital audio-visual applications and services. The purpose of DAVIC is to identify, select, augment, and develop internationally agreed specifications of open interfaces and protocols that maximize interoperability across countries and applications/services. ITL works with DAVIC members on the interoperability testing of digital video products conforming to DAVIC specifications. These efforts concentrate on the development of conformance test suites and establishment an interoperability testbed where developers could test their products. The ITL principal is David Su.

Forum of Incident Response and Security Teams (FIRST)

This international, government/industry/academia coalition was formed to share information on information security vulnerabilities and attacks. ITL participates as a member of the FIRST steering committee. John Wack and Marianne Swanson represent ITL in this interaction.

Information Infrastructure Standards Panel (IISP)

The Information Infrastructure Standards Panel (IISP) was created by ANSI to identify critical standards requirements for the emerging Global Information Infrastructure (GII). The work of IISP will lead to the creation of standards that will enable the growth of the GII and help bring about interoperability between GII components developed within different industries. As such, the IISP is predominantly made up of representatives from industry. ITL has contributed to the fulfillment of IISP's mission by devising a conceptual Framework to guide the process of identifying standards requirements and assisting IISP members in the use of this Framework. Christopher Dabrowski is the ITL contact.

Information Infrastructure Task Force (IITF) Committee on Applications and Technology (CAT)

The CAT, led by NIST Director Arati Prabhakar, is responsible for coordinating the Administration's efforts to develop, demonstrate, and promote applications of information technology in specific application areas. ITL works with the CAT working groups and CAT participants in various government agencies and with industry and academia to develop publications, conduct meetings and conferences, distribute both print and electronic information, and respond to queries about the NII and the GII. One resource provided is the NII Virtual Library Home Page found at http://nii.nist.gov, co-sponsored with the private sector Council on Competitiveness. Judi Moline is the ITL contact.

Information Technology Industry Council (ITI)

ITL has an informal relationship with the Information Technology Industry Council (ITI). One of ITI's activities is to develop positions on issues in standards, testing, certification and quality assurance. Areas include ergonomics, health, safety and hardware, software and systems functional and performance characteristics. ITI also serves as the secretariat for the American National Standards Institute (ANSI) Accredited Standards Committee X3 (Information Technology) and as U.S. Technical Advisory Group (TAG) administrator for ISO/IEC Joint Technical Committee 1 on Information Technology. The ITL liaison to ITI is Michael D. Hogan.

Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers, Inc. is the world's largest technical professional society, promoting the development and application of electrotechnology and allied sciences for the benefit of humanity and the advancement of the profession. ITL maintains close ties with the IEEE to help IEEE identify forward-looking standards efforts and to provide industry input to ITL's program planning for standards and test activities. IEEE's close ties to industry and to academia help ITL to understand industry needs and requirements; to know about academic research in areas of interest to NIST; and to communicate about ITL projects. Daniel R. Benigni is Vice President for Professional Activities and Chairman of the United States Activities Board (IEEE-USA) for 1997.

Interactive Multimedia Association (IMA)

As multimedia applications and objects proliferate on the Internet, standard methods for describing and registering objects will be needed for users and suppliers to easily locate, use, distribute, buy, and lease these objects for their applications. ITL is collaborating with the IMA and other industry and government groups to develop a metadata standard for multimedia objects (i.e., object containing text, graphics, audio, video), initially in the educational learning domain to demonstrate the metadata concept with educational objects in an Internet, Web-based environment. The project is expected to lead to standards for describing multimedia objects using standard metadata descriptions, and identifying other relevant object information through an object registry. ITL will host a pilot system implementation and demonstration at NIST later in 1997. Tom Rhodes coordinates the project for ITL.

International Information Integrity Institute (I4)

This internationally based membership organization of information technology security managers consists of the senior security managers from large, international organizations. NIST is a U.S. Government representative in I4. I4 is managed by SRI International (previously, Stanford Research Institute), which conducts meetings (four per year), produces regular technical reports, and undertakes special research projects. In October 1996, NIST hosted Forum 29, one of four yearly conferences sponsored by I4. The conference focused on electronic commerce security and brought together over 200 specialists from the U.S. and overseas. Stuart Katzke is the ITL contact.

International Multimedia Teleconferencing Consortium (IMTC)

The IMTC is a non-profit corporation founded to promote the creation and adoption of international standards for multipoint document and video teleconferencing. The IMTC and its members promote a "Standards First" initiative to guarantee interworking for all aspects of multimedia teleconferencing. The concentration of this group is on promoting and facilitating the broad use of multimedia teleconferencing based on open standards, including the standards adopted by the ITU. Jean-Philippe Favreau is the principal ITL contact for these activities.

Internet Engineering Task Force (IETF)

ITL contributes to the technical development of the Internet through its participation in the Internet Engineering Task Force (IETF). The IETF develops standards for internetwork technology and for evolving the Internet Protocol Next Generation (IPng). ITL contributes in the areas of IPv6, IPv4 security, integrated services, systems management, and routing. Additionally, Doug Montgomery co-chairs the IETF interdomain-system-to-interdomain-system (IS-IS) for IP Internet Working Group. Rob Glenn is the contact for non-security related IPv6 work. John Wack works in the IPv6 security and key management areas and Tim Polk serves on the IETF PKIX Working Group which addresses Public Key Infrastructure (PKI) issues.

National Information Infrastructure Advisory Council (NIIAC)

The NIIAC was formed to provide guidance to the Secretary of Commerce and the interagency Information Infrastructure Task Force (IITF) on the development of the National Information Infrastructure. The NIIAC was a 37-member advisory panel composed of individuals representing private industry, labor, state and local governments, public interest organizations, academia, and leading experts in NII-related fields. The NIIAC was established in January 1994 and completed its work in February 1996.

National Information Infrastructure (NII) Awards

Sponsored by over 60 groups from industry, government, and community leaders, the NII Awards recognize innovation and excellence in the use of networked information technology. As the representative of the interagency Information Infrastructure Task Force, ITL provided guidance to NII Awards organizers during the inaugural campaign in 1994-95 and continued to provide support in 1996. Judi Moline is the ITL contact.

National Software Council (NSC)

Incorporated in April 1995, the NSC is a nonprofit membership organization composed of industry, academia, and government members. Its mission is to ensure that the U.S. software industry continues to make a strong and growing contribution to national economic prosperity. ITL staff participated in NSC planning meetings over the past two years to define the scope and direction of the organization. As a government affiliate member of NSC, ITL obtains current information about industry and government technology requirements. Dolores Wallace and Tom Rhodes are the ITL representatives; Rhodes serves on the Executive Committee of the NSC.

Network Management Forum (NMF)

ITL worked with industry consortia to develop OMNI*Point* specifications, as defined by the Open Management Roadmap partnership for addressing the full range of network management requirements. Released in Fall 1992, OMNI*Point* 1 was the first in a series of incremental specifications intended to provide a common approach to the integration and management of diverse technologies. Fran Nielsen serves as Secretary of the User Advisory Council of the OMNI*Point* and is the ITL participant in the NMF.

NII Testbed Consortium (NIIT)

NIST holds membership in the NIIT consortium, an industry, government, and academia collaboration to develop an advanced, nationwide information testbed that will deliver applications to solve real-world problems. Application working groups include Healthcare, Earth and Environmental Sciences, Electronic Commerce, Astrophysics, and Manufacturing. The NIST Concurrent Engineering project is a five-year project that will use currently available high performance computing and communication (HPCC) technologies to develop a platform capable of demonstrating the practical uses of HPCC technologies in concurrent engineering. ITL's participation in the consortium ensures that the NIST Concurrent Engineering project will be closely linked with industry efforts to focus on actual industry needs and to ensure maximum benefit from the NIST efforts. Shukri Wakid is the principal NIST participant.

Object Management Group (OMG)

The OMG is a nonprofit international consortium, based in Framingham, Massachusetts, of over 500 organizations whose mission is to research, develop, and promote the use of object oriented technology for distributed systems development. The membership consists of all the major producers of information technology hardware and software (e.g., IBM, DEC, Sun, Microsoft), large user organizations e.g., Boeing, Bellcore, Merrill Lynch, Citibank, GTE, MCI, British Telecom), government agencies (e.g., NASA, NSA, DISA, NIH), and universities (e.g., MIT, Stanford, University of Illinois, University of Michigan). Over the past year, NIST representatives from ITL and the Manufacturing Engineering Laboratory attended OMG meetings as part of joint project with DISA and Sematech to develop an open, distributed framework for semiconductor manufacturing. John Barkley is ITL's technical point of contact in the OMG.

Open Group

Created by the recent merge of X/Open and the Open Software Foundation (OSF), the Open Group provides a forum for vendors to discuss and establish consensus on open system specifications. A member of the former X/OPEN User Council for several years, ITL works closely with this group in the development of conformance testing technology for information systems. We maintain an informal relationship with the former OSF, an international organization dedicated to the development and delivery of an open, portable software environment to which vendors and users have equal input and access. OSF efforts address the need for portability, interoperability, and scalability. The organization made their Distributed Computing Environment (DCE) technology available for use in our distributed systems engineering work.

Society for Information Display (SID)

This worldwide professional society and forum is committed exclusively to the advancement of information display technologies. Membership in SID entitles ITL to participate in SID-sponsored symposia, seminars, and access to SID publications. John Roberts is the principal contact.

Software Engineering Institute (SEI)

Established by Congress in 1984, the SEI is a research and development center with a broad charter to address the transition of software engineering technology. ITL established a memorandum of understanding (MOU) with SEI to work collaboratively on software engineering issues of mutual interest. Under this agreement, ITL and SEI worked together to address issues and develop standards for integrated software engineering environments. SEI also participated with ITL in the formation of the Center for High Integrity Software Systems Assurance. An ITL staff member served on SEI's Educational Products Advisory Board with representatives from Texas Instruments, AT&T, Carnegie Mellon University, Rochester Institute of Technology, and the Department of the Army.

Software Productivity Consortium (SPC)

An industry-based consortium founded in 1985, the SPC focuses on advancing the fundamental processes and methods of software and systems engineering technologies for developing high-quality software intensive systems. The SPC provides a forum for ITL to collaborate with industry, government, and academia on development, application, and exchange of advanced software processes and methods for developing high-quality software systems. The forum allows ITL to contribute its technical views, program results, and capabilities to various industry sectors and provides a mechanism for technology exchange and further collaboration with industry. Tom Rhodes represents ITL in this consortium.

Telecommunications Industry Association (TIA)

The TIA is a major developer of voluntary standards for telecommunications products and the principal U.S. developer for fiber optic standards, building wiring standards, and cellular telephony standards. Bill Burr, who serves as Chairman of the Federal Wireless Policy Committee subcommittee on Privacy and Authentication, attends meetings of the TIA TR 46 (committee on Personal Communications Systems) ad hoc on Privacy and Authentication and the TIA TR 45 (committee on cellular telephony) Ad Hoc Authentication Group (AHAG) to reflect federal security concerns about wireless and cellular communications.

Video Electronics Standards Association (VESA) Special Interest Group (SIG) on Flat Panel Displays

ITL's Workshop on the Computer Interface to Flat Panel Displays, held in San Jose, California, in January 1994, resulted in a consensus to form a VESA SIG to undertake the development of a standard or series of standards for the interface between a flat panel display and its controller. This interface standard addresses both active and passive flat panel displays in integrated devices, and will cover both the electrical and the mechanical specifications. As a full member of VESA, ITL participates in the technical development of standards and develops laboratory implementations of proposed interface architectures by developing laboratory metrics. The ITL contact is John Roberts.

SELECTED COLLABORATIONS

ITL works with industry, government, and academia to pursue research and development projects of mutual interest, including the following:

Calibration Software

ITL software proved to be a crucial factor in resolving unexplained accuracy issues discovered in the calibration process and equipment at Image Guided Technologies, Inc., a Boulder, Colorado, firm that designs, manufactures, and sells three-dimensional optical localizers for medical and industrial applications. Their localizer is used primarily in neurosurgery to allow a surgeon to track the location of a probe within a patient's skull. Obviously, such localizers must be calibrated to a very high degree of accuracy.

ODRPACK, software developed by ITL's Mathematical and Computational Sciences Division, is uniquely well-suited for modeling three-dimensional data such as the data produced by localizers. By applying ODRPACK to their problem, Image Guided Technologies was able to find and correct problems with their process. In addition, ODRPACK enabled them to develop new models for the optical properties of their system. Now, every system they ship is tested and certified for accuracy using software built on ODRPACK.

ODRPACK solves the extended nonlinear least squares problem where both the explanatory as well as the dependent variables have errors, a procedure sometimes known as Orthogonal Distance Regression. ITL developed the algorithm and the software, which is available using the NIST Guide to Available Mathematical Software (GAMS) (http://gams.nist.gov/). Janet Rogers is the ITL contact.

Electronic Signatures

ITL recently completed a three-phase, multi-year project with the U.S. Army Corps of Engineers to implement electronic signatures in the Corps of Engineers Financial Management System (CEFMS). The final report, which includes a number of short- and long-term recommendations, is being used by the General Accounting Office (GAO) as it considers a sanctioning of CEFMS.

CEFMS is a Corps-wide system that migrates numerous financial applications, such as purchase requests, obligations, disbursement, and travel order certification, to a completely electronic format. Corps employees generate unique electronic signatures on electronic forms, and other CEFMS users electronically verify the correctness of those signatures, eliminating the need to generate paper-based forms with handwritten signatures. The subsystem of CEFMS that provides this signature generation and verification capability is the Electronic Signature System (ESS). In 1992, ITL designed the technical specifications for the Army Corps' Request for Proposal (RFP) for the ESS, implementing the Data Encryption Standard algorithm, key notarization techniques, cryptographic service calls (CSCs), and a software reference implementation of many ESS functions.

Approximately 5,000 CEFMS users currently use the EES, and it is anticipated that over 40,000 Corps personnel will eventually use the system. The ESS was designed to be a modular system that can be implemented by other government agencies. For example, the Department of State recently adopted the ESS to enhance security in an inter-embassy financial application. Participants in the project included the U.S. Army Corps of Engineers, two of the Corps' contractors (Gradkell Systems Inc. and Litronic), the General Accounting Office, and ITL staff members Jim Foti, Sharon Keller, and Donna Dodson.

Usability Engineering

In February 1996, ITL sponsored a Symposium on Usability Engineering: Industry-Government Collaboration for System Effectiveness and Efficiency. The symposium brought together about 100 industry and government representatives to exchange information and strategies for achieving effectiveness, efficiency, and satisfaction in computer-based government systems. Attendees included project development managers, government contractors, procurement officials, analysts and engineers, technical staff and researchers, commercial off-the-shelf (COTS) product vendors, consultants, and policy makers.

In designing new government computer systems and in redesigning legacy systems, industry and government must be aware of the best practices now available to ensure the usability of such systems. Topics covered at the symposium included an introduction to usability engineering, usability trends in government, success stories, costs and benefits, standards and guidelines, industry strategies and practices, special issues for complex systems, and making usability work in the organizations. Laura Downey coordinated the conference for ITL.

Support for Automotive Industry

A major barrier to increasing the efficiency of U.S. manufacturers is the hesitance of small and medium-sized enterprises (SMEs) to adopt the advanced information technologies required to conduct business electronically. On April 30, 1996, ITL coordinated a meeting with automotive industry executives on behalf of the Department of Commerce Under Secretary for Technology to address the issue of information technology adoption by SMEs. Attendees included executives from Chrysler Corporation, the Automotive Industry Action Group, the Industrial Technology Institute, and NIST manufacturing experts. This gathering was the first of a planned series of meetings with representatives of the "Big Three" automakers to discuss what can be done to accelerate the use of advanced information technologies by the suppliers that do business with large manufacturers. Judi Moline is the ITL contact.

Statistics in Quality, Industry, and Technology

ITL hosted the 13th Quality and Productivity Research Conference and the 3rd Spring Research Conference on Statistics in Industry and Technology at NIST from May 29-31, 1996. The goal of the conference was to stimulate interdisciplinary research among statisticians, engineers, and physical scientists in quality and productivity, with a focus on industrial needs, specifically in the physical and engineering sciences. Statistical issues and research approaches drawn from collaborative research were highlighted. The audience consisted of approximately 200 statisticians, engineers, and quality professionals. The conference was sponsored jointly by NIST, E.I. du Pont de Nemours & Company, the American Statistical Association, and the Institute of Mathematical Statistics. Eric Lagergren coordinated the conference for ITL.

Video-on-Demand Interoperability Testing

ITL participated in the Digital Audio Visual Council (DAVIC) Interoperability Test Event at the Image Technology for New Media Center at Columbia University in New York City. The event was held in parallel with the 13th DAVIC meeting. DAVIC is an international consortium established to develop specifications for, and to promote interoperability of, digital video applications.

On the first day, more than 200 people viewed the demonstration of the Video-on-Demand (VoD) Interoperability Test Laboratory facility constructed by ITL. The purpose of the test event was to show that DAVIC-compliant equipment could interoperate. A total of eight companies from the U.S., Europe, and Japan participated in the event, interconnecting their VoD components, video server and Set-Top-Unit (STU), via an ATM network. Equipment used in the demonstration consisted of prototype implementations using either workstations or high-end personal computers (PCs). The STUs from other participants successfully accessed ITL's video server, and ITL's STU interoperated with Columbia's server. ITL announced at the closing plenary of the DAVIC meeting that we are ready to conduct interoperability tests with other parties at its laboratory. David Su is the ITL contact.

Electronic Statistical Handbook

ITL statisticians joined forces with SEMATECH to produce an electronic statistical handbook. To be disseminated via the Internet, the handbook will provide access to modern statistical and graphical techniques for solving engineering problems. A demonstration for the SEMATECH Advisory Council focused on integration between viewing the handbook with a Web browser and doing real-time computations with the public domain software package Dataplot. The Council supported the project and provided reviewers from the member companies for individual chapters of the electronic handbook. Carroll Croarkin coordinates the project for ITL.

Sparse Matrix Software

As part of the ongoing standardization efforts of the Basic Linear Algebra Subprogram (BLAS) Technical Forum, ITL announced a software package for low-level sparse matrix computations for public review. The NIST Sparse BLAS package consists of over 1,300 routines supporting linear algebra for various sparse matrix storage schemes.

Many physical modeling and simulation problems give rise to large sparse linear systems, and these are frequently the computational bottleneck of an application code. The availability of efficient low-level BLAS routines is therefore of keen interest to computational scientists and scientific computing vendors.

The BLAS Technical Forum is a multidisciplinary group with commercial participants (IBM, Digital Equipment Corporation, Cray Research) as well as participants from universities and research centers. The Forum is working on the establishment of interface standards to enable libraries for sparse and parallel linear algebra computation to interoperate easily and efficiently.

More information about the NIST Sparse BLAS effort can be found at "http://math.nist.gov/spblas". Roldan Pozo and Karin Remington are the ITL contacts.

Public Key Infrastructure (PKI)

ITL established cooperative research and development agreements (CRADAs) with industry partners to develop a minimum interoperability specification for organizations to use in building PKI components. Industry partners included AT&T Government Markets, BBN Corporation, Certicom Corporation, Cylink Corporation, DynCorp Information & Engineering Technology Inc., Information Resource Engineering Inc., Motorola, Northern Telecom Ltd. (Nortel), SPYRUS Inc., and VeriSign Inc. Completed in the fall of 1996, the project resulted in a Minimum Interoperability Specification of PKI Components.

By working together to develop a PKI, industry and government users help to ensure that future PKI components from different manufacturers can interoperate. A PKI is essential to facilitate the use of digital signatures and other forms of public key cryptography by industry and government users of information systems. Donna Dodson and Noel Nazario coordinated the ITL effort.

Intelligent Collaboration and Visualization

On November 4, 1996, ITL hosted a working meeting of the Evaluation Working Group (EWG) of the DARPA Intelligent Collaboration and Visualization (IC&V) Program. Working with other EWG participants from MITRE, CMU, and the National Intelligence Mapping Agency, ITL is developing methodologies, metrics, and testing tools to evaluate generation-after-next collaboration systems and supporting infrastructural technologies. ITL's EWG efforts focus on the development of testing and instrumentation technology that will enable collaboration systems developed through the DARPA IC&V program to be evaluated in terms of objectives for task performance, scalability, heterogeneity, and interoperability. Doug Montgomery and Sharon Laskowski coordinate the project for ITL.

Prototype Conferencing Products Interoperability

More than 20 hardware and software firms, telephone companies, and network service providers participated in the recent Event-120, the industry's second interoperability testing event for providers of data conferencing products and services. The event tested T.120-compliant, multipoint data conferencing applications. Of more than 3000 tests performed, 95 percent resulted in successful links between vendors. Companies that participated in Event-120, sponsored by DataBeam and Lucent Technologies, included Accord Video Telecommunication, AT&T, ConferTech, DataBeam Corporation, Deutsche Telekom, ETRI, Future Labs, Intel Corporation, Lucent Technologies, MCI, Microsoft Corporation, MultiLink, OutReach Technologies, PictureTel, Polycom, SAT, Teles AG, VideoServer, VTEL Corporation and Zydacron.

The International Multimedia Teleconferencing Consortium, Inc. (IMTC) organized the event to facilitate the rapid development and delivery of T.120 standards-based conferencing products and services, and to continue promoting the importance of industry-wide interoperability as a base for building consumer confidence. Conferencing technologies are used in applications such as distance learning, telemedicine, corporate training, and working collaboratively with distant colleagues. T.120 applications currently include shared whiteboarding and multipoint file transfer. Consumer-oriented applications that require real-time, multipoint data delivery, such as multiplayer games, online chat programs, and virtual reality simulations, are also expected to incorporate the T.120 standards, a series of standards for real-time, multipoint data exchange. The evolving series, initially adopted by the International Telecommunication Union (ITU) in March 1995, continues to be extended. Programs such as Event-120 ensure that the standards are interpreted and implemented by different vendors in a way that advances industry-wide interoperability of their products. As has been proven with other successful technologies, such as electronic mail and fax machines, interoperability of products and services is essential to widespread acceptance.

A second test event was held concurrently, IMTC's third H.324 Interoperability Test Event, sponsored by Intel. Testing vendors included 8x8, Inc., Acer Advanced Labs, Inc., Creative Labs, Inc., Intel Corporation, Lucent Microelectronics, Multimedia Access Corporation, RSA Communications Inc. (Cirrus Logic), Smith Micro (Video Products Division), Sony, Teles AG, VDOnet Corporation, Vivo Software, and Winbond Systems Lab. During the session, participants performed structured interoperability tests between products based on the ITU-T H.324 standard for videoconferencing. H.324 protocols tested were G.723, H.263, H.245 and H.223. Jean-Philippe Favreau is the ITL contact.

Cooperative Research and Development Agreements

Through Cooperative Research and Development Agreements (CRADAs), we establish partnerships with industry, academia, and government to pursue mutual areas of research. Our technical staff worked with the following 53 organizations in 1996:

Research Partner	Project
Adobe Systems Incorporated	PostScript Language, PDF Format and Acrobat Software Review
Cray Research, Inc.	Alternative Computer Arithmetics
Enterprise Integration Technologies	Develop Software and Services for Electronic Commerce on the Internet
Linguistic Data Consortium	Corpora to Support Human Language Technology Research
MicroFab Technologies	Solder Jet Science and Technology
SoHaR Incorporated	Standard Reference Material for Software Error, Fault, Failure Data — Collection & Repository

The following CRADA partners collaborated with us on the Development of Interoperable Public Key Infrastructure Specifications:

AT&T Government Markets
BBN Corporation
CERTICOM Corporation
Cylink Corporation
Dyncorp Inc.
IRE, Inc.
Motorola
Northern Telecom
SPYRUS, Inc.
VeriSign Inc.

The North American ISDN Users' Forum (NIUF) is an industry/government forum established in 1988 to create a strong user voice in the implementation of ISDN applications. In 1996, CRADA partners were:

ADTRAN
AHK & Associates
American Computer & Electronics Corporation
Ameritech Services
AT&T Bell Laboratories
Bell Atlantic Network Services, Inc.
Bell Communications Research
BellSouth
Century Telephone Enterprises, Inc.
Defense Communication Agency
Electronic Data Systems Corporation
Fujitsu Networks Industry, Inc.
General DataComm, Inc.
GTE Southwest Incorporated
Hayes Microcomputer Products, Inc.
Intecom, Inc.
International Business Machines Corporation
Lucent Technologies
Network Communications Corporation
North Carolina State University
Northern Telecom Inc.
NYNEX
Open Communications Networks, Inc.
Presearch, Inc.
RLR Resources
Siemens Stromberg-Carlson
Southwestern Bell Telephone Company
Symbolic Systems, Inc.
TASC (The Analytic Sciences Corporation)
Telamon, Inc.
Teltone Corporation
U.S. Air Force (Technology Integration Center)
U.S. Coast Guard
U.S. West
Unisys Corporation
West Virginia University
Xyplex, Inc.

GUEST RESEARCHERS

Guest Scientists and Research Associates **71**

Organizations represented include:

- Al-Akhamayn University
- American National Standards Institute
- Bhabha Atomic Research Center
- Department of Defense
- Electronics and Telecommunications Research Institute, Korea
- Environmental Protection Agency
- Flinders University
- George Mason University
- George Washington University
- Institut National des Telecommunications, France
- Korea Telecom Research Laboratories
- Los Alamos National Laboratory
- Ministry of Information and Communications, Taiwan
- National Aeronautics and Space Administration
- National Science Foundation
- National Security Agency
- Purdue University
- Space Science and Technology Center, People's Republic of China
- Syracuse University
- Trusted Information Systems, Inc.
- University of Maryland, Baltimore
- University of Maryland, College Park
- University of Nancy, France
- University of South Florida
- University of Texas at Austin
- University of Twente, The Netherlands
- VDG, Inc.

Faculty Appointments **27**

Colleges and universities represented include:

- Arizona State University
- Colorado State University
- Columbia University
- George Mason University
- Howard University
- Loyola College
- Old Dominion University
- Temple University
- University of Maryland, Baltimore Campus
- University of Maryland, College Park
- University of North Carolina
- University of Tennessee
- West Virginia University

INTERNATIONAL ACTIVITIES

Assistance to Singapore Government

ITL assisted the Singapore National Computer Board in reviewing and updating their information technology security standards. Stuart Katzke and Dennis Steinaur, Computer Security Division, provided the technical assistance.

ATM Network Technology

Through a Memorandum of Understanding, ITL, the Korean Telcom Research Group (KTRG), and the Electronics and Telecommunications Research Institute (ETRI) are jointly developing abstract conformance test and interoperability test suites for the ATM network protocols and Video-on-Demand (VoD) service. KTRG and ETRI assigned guest scientists to work at NIST in developing test suites and VoD reference implementations.

Collaboration with Electrotechnical Laboratory (ETL), Japan

As part of an ongoing ITL-ETL study on computer performance, Roldan Pozo spent two weeks as Visiting Scientist at the Electrotechnical Laboratory (ETL) in Tsukuba, Japan in February at the invitation of the Japanese Ministry of International Trade and Industry. Pozo presented four lectures on iterative methods for solving large sparse linear algebraic systems, object-oriented software design for scientific computing, and performance modeling of multifrontal methods for distributed memory architectures. The lectures took place at ETL, Fujitsu Laboratories, the KEK High-Energy Physics Colloquium, and the Performance Measurement Consortium in Tokyo. At Fujitzu, Pozo viewed a demonstration of the company's next-generation parallel computers.

Collaboration with Russian Academy of Sciences

As part of an international agreement between ITL and the Russian Academy which fosters scientific exchanges, Daniel Lozier hosted a six-week visit to NIST in October-November 1995 by Dr. J.M. Rappoport of the Russian Academy. Rappoport has published algorithms and software for special function evaluation, mostly in the Russian literature. During his visit, Dr. Rappoport began a collaboration with ITL scientists on algorithms for the MacDonald (modified Bessel) functions. These arise as the Kernel of the Kontorovich-Lebedev integral transform, for which little software exists in Western computer libraries.

Common Criteria (CC)

To improve the metrics and methods required to specify, build, and evaluate advanced information technology (IT) security products and systems, ITL is collaborating with Canada, France, United Kingdom, Germany, and the Netherlands to develop a common criteria that is flexible, extensible, responsive to market forces, and accepted by the major western economic powers. The CC is a comprehensive framework and technical criteria for defining and evaluating the security of IT products and systems. Specific activities include a North America-Europe effort to develop a harmonized CC and the conduct of trial evaluations to validate the CC. Another project, funded by the Defense Advanced Research Projects Agency, compares evaluations of the Trusted Mach Operating System against the European Information Technology Security Evaluation Criteria. The evaluations are being conducted by United Kingdom and German commercially licensed evaluation laboratories.

Cryptographic Applications Program Interfaces

In December 1994, ITL sponsored a workshop to address the growing interest in developing a generic Cryptographic Applications Program Interface (CAPI) and the need for convergence in the development of standards. This work is a collaborative effort with the United Kingdom (UK) Ministry of Defence, the National Security Agency, several standards organizations, and some commercial vendors. Officials from the UK and Canada shared their experiences with CAPI initiatives in their countries, and all participants agreed to coordinate future activities in this effort. A second meeting was held in March 1996, and periodic information exchanges continue.

Cryptographic Module Validation

ITL and the Communications Security Establishment of the Government of Canada collaborated on the development of the Cryptographic Module Validation Program, announced jointly on July 17, 1995. Products validated by this program as conforming to FIPS 140-1, *Security Requirements for Cryptographic Modules*, are accepted for use in both the U.S. and Canada for the protection of sensitive, unclassified information.

G-7 Global Information Society Inventory Pilot Project

Under the coordination of the European Community and Japan, the Global Inventory Project (GIP), one of eleven pilot projects designed to stimulate global applications of information technologies, aims to produce a multimedia inventory of national and international projects, studies, and calls relevant to the promotion and further development of knowledge and understanding of the information society. As the U.S.A.'s point of reference, ITL established an entry point for a sampling of current and proposed U.S. information infrastructure projects under ten application areas defined by the G-7 nations. Electronic project submission and access to the resources are available via the U.S. National Information Infrastructure Virtual Library Home Page at URL http://nii.nist.gov/.

G-7 Pilot Project on Global Electronic Commerce

Along with Japan and the European Community (EC), the Department of Commerce was designated the lead agency in a G-7 Information Society Pilot Project "Global Marketplace for Small and Medium Enterprises (SMEs)." The SME project seeks to identify the information needs of SMEs, promote SME use of the information infrastructure, and encourage the development and demonstration of electronic marketing, cooperation, and trade. The Department of Commerce and CommerceNet Consortium hosted a G-7 Working Group meeting in San Jose, California, in September 1995, at which ITL participated in the demonstration of the G-7 "Global Marketplace" server.

International Public Sector Information Technology (IPSIT) Group

IPSIT is an informal association of representatives of public sector organizations that identify, discuss, share experiences and raise awareness on issues in information management and technology in an informal and candid way with a view to encouraging action and resolution. IPSIT discusses topics of mutual interest from the perspective of national solutions. Areas of interest include common information and communications architectures, interconnectivity, information exchange, use of standards, and publicly available specifications. Participation includes representatives from Australia, Canada, Germany, Italy, Japan, Korea, Portugal, South Africa, Sweden, Switzerland, the UK, and the U.S. ITL participates as a representative of the U.S. Government.

International Statistics Institute (ISI)

Raghu N. Kacker, Statistical Engineering Division, was elected an Ordinary Member of the ISI in 1995. With fewer than 2000 members representing 96 countries, the ISI elects fewer than 100 new members annually.

Organization for Economic Cooperation and Development (OECD)

Based in Brussels, Belgium, the OECD is associated with the European Community (EC). ITL participated in the OECD Cryptography Experts Group in discussions on the development of cryptography principles. Edward Roback represented ITL in this effort.

Technical Support to Jordan

At the Middle East and North Africa (MENA) Summit held in Amman, Jordan, in November 1995, three ITL staff members participated in the demonstration of the use of the Internet (recently named MENA-PeaceNet) to foster commerce and other peaceful activities in the Middle East. A satellite link was installed in Amman to connect to the U.S. and a microwave link was added to provide connectivity to one of the hotels where the ministers were to meet. A special demonstration to show some of the features of the Internet was arranged for the ministers of the countries signatory to Middle East Peace agreements (Taba Ministers) including Egypt, Israel, Jordan, and the Palestinian Authority. The system was operated for the duration of the Summit.

Follow-on meetings were held at the International Trade Administration (ITA) of the Department of Commerce. Our staff also participated in meetings with representatives of Egypt, Jordan, Israel, and the Palestinian Authority, in Amman, Jordan; with representatives of the Middle East and North African (MENA) Secretariat, in Rabat, Morocco; and with representatives of the World Economic Forum (WEF) in Geneva, Switzerland. The meetings resulted in plans to set up skeleton Web pages to permit each participating country to enter information about its geography, its trade requirements, and its programs, its industrial activities, its products, and other commercial activity. Web pages were prepared and installed on a NIST server (URL=mena-peacenet.nist.gov). In addition, ITL also provided six e-mail reflectors. The new Web site and e-mail reflectors were presented to the TABA Ministers at the MENA Summit in Cairo, Egypt, held November 12-14, 1996.

World Summit on Trade Efficiency

In November 1994, four computer scientists participated in the World Summit on Trade Efficiency as part of the Official U.S. Delegation. ITL demonstrated a pilot electronic commerce SmartProcurement system jointly developed with the Enterprise Integration Technologies Corporation. The SmartProcurement system is an innovative application of two evolving computer technologies, the WWW and Intelligent Agents, and reduces bid time from vendors to hours instead of days or weeks.

Worldwide Electronic Commerce: Law, Policy, Security and Controls Conference

In October 1995, ITL participated as an affiliated cosponsor of an international conference on issues of electronic commerce and the law. About 300 industry, government, and foreign participants attended. Other cosponsors included the American Bar Association; the Centre for Commercial Law Studies, Queen Mary & Westfield College, UK; EDI Association of the UK; Harvard Law School, International Union of Latin Notaries; International Chamber of Commerce, Paris; Software Publishers Association; United Nations Commission on International Trade Law; and the U.S. Council of International Business.

PATENTS

In 1996, ITL researchers applied for five new patents, bringing to six the number of patents pending. Nine patents have been issued to date:

- Cryptographic Key Notarization Methods and Apparatus
  Miles Smid and Dennis Branstad
  Issued May 31, 1983

- Satellite Controlled Digital Clock System
  Joseph Cateora, Dick Davis, and D. Hanson
  Issued March 29, 1977

- Object/Anti-Object Neural Network Segmentation
  Charles Wilson, Michael Garris, and R. Wilkinson
  Issued September 14, 1993

- Method and Apparatus for Analyzing Character Strings
  Jon Geist
  Issued July 12, 1994

- Automated Recognition of Characters Using Optical Filtering With Positive and Negative Functions Encoding Pattern and Relevance Information
  Charles Wilson
  Issued November 1, 1994

- Automated Recognition of Characters Using Optical Filtering With Maximum Uncertainty Minimum Variance (MUMV) Functions
  Charles Wilson and James Blue
  Issued December 6, 1994

- Apparatus For Identifying Unknown Words By Comparison to Known Words
  Jon Geist
  Issued February 21, 1995

- Procedure for Digital Image Restoration
  Alfred S. Carasso
  Issued May 9, 1995

- Aerosol Mass Spectrometer
  Kensei Ehara
  Issued June 27, 1995

Publications

October 1994 - December 1996

NIST Publications are available from the Government Printing Office (GPO) at (202) 512-1800 or the National Technical Information Service (NTIS) at (703) 487-4650. SN numbers are stocked by GPO; PB numbers are stocked by NTIS. Our NIST Publications List 88, *Information Technology Publications and Products*, is available online at http://www.itl.nist.gov. Click on Products, then click on Publications (at bottom of screen).

NIST Special Publication — Title

STANDARD REFERENCE MATERIALS SERIES

260-125 Statistical Aspects of the Certification of Chemical Batch SRMs
By S.B. Schiller
July 1996 PB96-210877 $21.50

NIST INFORMATION TECHNOLOGY SERIES

500-220 *Guide on Open System Environment (OSE) Procurements*
By Gary Fisher
October 1994 PB95-169496 $31.00

500-221 *A User Study: Informational Needs of Remote National Archives and Records Administration Customers*
By Judi Moline and Steve Otto
November 1994 PB95-154738 $25.00

500-222 *Glossary of Software Reuse Terms*
By Susan Katz, Christopher Dabrowski, Kathryn Miles, and Margaret Law
December 1994 PB95-178992 $19.50

500-223 *A Framework for the Development and Assurance of High Integrity Software*
By Dolores R. Wallace and Laura M. Ippolito
December 1994 PB95-173084 $21.50

500-224 *Stable Implementation Agreements for Open System Environment, Version 8, Edition 1*
December 1994 (supersedes NIST SP 500-214)
Albert Landberg, Workshop Chairman; Joseph Hungate, Workshop Vice Chairman; and Brenda Gray, Editor
December 1994 Available on CD-ROM at (202) 371-1013.

NIST Special Publication	Title		
500-225	*Overview of Third Text Retrieval Conference (TREC-3)*		
	D. K. Harman, Editor		
	April 1995	PB95-216883	$67.00
500-226	*Self Monitoring Accounting Systems*		
	By Roger F. Sies		
	March 1995	PB95-216602	$19.50
500-227	*ELECTRONIC ACCESS: BLUEPRINT for the National Archives and Records Administration*		
	By Judi Moline and Steve Otto		
	April 1995	SN003-003-03330-8	$4.50
500-228	*Guidelines for the Evaluation of X.500 Directory Products*		
	By John Tebbutt		
	May 1995	PB95-231908	$21.50
500-229	*Z39.50 Implementation Experiences*		
	Paul Over, William E. Moen, Ray Denenberg, and Lennie Stovel, Editors		
	September 1995	PB96-114939	$28.00
500-230	*Application Portability Profile (APP) The U.S. Government's Open System Environment Profile Version 3.0*		
	By Gary E. Fisher		
	February 1996	SN003-003-03389-8	$7.00
500-231	*Guidelines for the Evaluation of Electronic Data Interchange Products*		
	By John J. Garguilo and Paul Markovitz		
	February 1996	SN003-003-03382-1	$4.25
500-232	*Open System Environment (OSE): Architectural Framework for Information Infrastructure*		
	By Frederick (Fritz) Schulz		
	December 1995	SN003-003-03380-4	$3.75
500-233	*A Manager's Guide for Monitoring Data Integrity in Financial Systems*		
	By Roger Sies		
	February 1996	SN003-003-03387-1	$5.00
500-234	*Reference Information for the Software Verification and Validation Process*		
	By Dolores R. Wallace, Laura Ippolito, and Barbara Cuthill		
	April 1996	SN003-003-03410-0	$6.50
500-235	*Structured Testing: A Testing Methodology Using the Cyclomatic Complexity Metric*		
	Dolores Wallace, Editor; A. H. Watson and T.J. McCabe		
	August 1996	SN003-003-03426-6	$13.00
500-236	*Overview of the Fourth Text REtrieval Conference (TREC-4)*		
	Donna K. Harman, Editor		
	October 1996	SN003-003-03430-4	$59.00

NIST COMPUTER SECURITY SERIES

800-10 *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*
By John P. Wack and Lisa Carnahan
December 1994 PB95-182275 $21.50

800-11 *The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security*
By Karen Olsen and John Tebbutt
February 1995 PB95-189445 $19.50

800-12 *An Introduction to Computer Security: The NIST Handbook*
By Barbara Guttman and Edward Roback
October 1995 SN003-003-03374-0 $18.00

800-13 *Telecommunications Security Guidelines for Telecommunications Management Network*
By J. Kimmins, C.R. Dinkel, and D.L. Walters
October 1995 SN003-003-03376-6 $3.50

800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*
By Marianne Swanson and Barbara Guttman
September 1996 SN003-003-03423-1 $7.50

NIST FEDERAL IMPLEMENTATION CONVENTIONS FOR ELECTRONIC DATA INTERCHANGE SERIES

881-1 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 838 Trading Partner Profile (Vendor Registration), Implementation Convention*
Jean-Philippe Favreau, Editor
August 1995 SN003-003-0336304 $4.25

881-2 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 838 Trading Partner Profile (Confirmation of Vendor Registration), Implementation Convention*
Jean-Philippe Favreau, Editor
August 1995 SN003-003-03364-2 $1.75

881-3 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 850, Award Instrument, Implementation Convention*
Jean-Philippe Favreau, Editor
August 1995 SN003-003-03365-1 $14.00

NIST Special Publication	Title
881-4	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 860, Modifications to Award Instrument, Implementation Convention* Jean-Philippe Favreau, Editor August 1995 SN003-003-03366-9 $15.00
881-5	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 865 Purchase Order Change Acknowledgment/Request - Seller Initiated, Implementation Convention* Jean-Philippe Favreau, Editor February 1996 SN003-003-03397-9 $11.00
881-6	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 855 Purchase Order Acknowledgment, Implementation Convention* Jean-Philippe Favreau, Editor February 1996 SN003-003-03398-7 $3.00
881-7	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 843 Response to Request for Quotation, Implementation Convention* Jean-Philippe Favreau, Editor February 1996 PB96-168984 $35.00
881-8	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 840, Request for Quotation, Implementation Convention* Jean-Philippe Favreau, Editor February 1996 SN003-003-03402-9 $13.00
881-9	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 836, Procurement Notices, Implementation Convention* Jean-Philippe Favreau, Editor February 1996 SN003-003-03400-2 $3.25
881-10	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 810, Invoice — [Commercial Invoice], Implementation Convention* Jean-Philippe Favreau, Editor November 1996
881-11	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 820, Payment Order/Remittance Advice, Implementation Convention* Jean-Philippe Favreau, Editor November 1996
881-12	*Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 855, Purchase Order Acknowledgement, Implementation Convention* Jean-Philippe Favreau, Editor November 1996

881-13 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 997, Functional Acknowledgement, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

881-14 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 864, Text Message, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

881-15 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 824, Application Advice, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

881-16 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 832, Price/Sales Catalog, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

881-17 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003050 Transaction Set 997, Functional Acknowledgement, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

881-18 *Federal Implementation Guideline for Electronic Data Interchange, ASC X12 003040 Transaction Set 840, Request for Quotation, Implementation Convention*
Jean-Philippe Favreau, Editor
November 1996

NIST SPECIAL PUBLICATIONS

857 *Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology*
Office of the Director, NIST; Kathleen Roberts, Editor
May 1994 SN003-003-03267-1 $7.00

868 *The Information Infrastructure: Reaching Society's Goals*
Office of the Director, NIST; Kathleen Roberts, Editor
September 1994 SN003-003-03283-2 $11.00

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) APPROVED 1995-96

To order FIPS, contact NTIS at (703) 487-4650.

FIPS No.	Category	Title-Date	Change Notices
8-6	(4) S	Metropolitan Areas (Including MSAs, CMSAs, PMSAs, and NECMAs) 95 Mar	2
10-4	(4) S	Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions 95 Apr	
21-4	(3) S	COBOL 95 Jan 23	
119-1	(3) S	Ada 95 Mar 13	
128-2	(3) S	Computer Graphics Metafile (CGM) 96 Apr 17	
146-2	(2&3) S	Profiles for Open Systems Inter-networking Technologies (POSIT) 95 May 15	2
153-1	(3) S	Programmer's Hierarchical Interactive Graphics System (PHIGS) 95 Jan 27	
161-2	(3) S	Electronic Data Interchange (EDI) 96 May 22	
172-1	(3) S	VHSIC Hardware Description Language (VHDL) 95 Jan 27	
177-1	(3) S	Initial Graphics Exchange Specification (IGES) 96 Apr 23	
179-1	(2&3) S	Government Network Management Profile (GNMP) 95 May 15	2
180-1	(5) S	Secure Hash Standard (SHS) 95 Apr 17	
193	(3) S	SQL Environments 95 Feb 3	

Pub. Number	Title	
194	(3) S	Open Document Architecture (ODA) Raster Document Application Profile (DAP) 95 Mar 13
195	(7) S	Federal Building Grounding and Bonding Requirements for Telecommunications 95 Aug 15
196	(5) S	Entity Authentication Using Public Key Cryptography (*Federal Register* Date)

CURRENT ITL BULLETINS

To request our bulletins or to be placed on our bulletin mailing list, call (301) 975-2817.

John Wack and S. Kurzban, *Computer Virus Attacks*, August 1990.

Edward Roback, *Computer Security Roles of NIST and NSA*, February 1991.

Roy Saltman, *Security Issues in the Use of Electronic Data Interchange*, June 1991.

Elizabeth Lennon, *The NIST POSIX Testing Program*, October 1991.

Jim Dray, *Advanced Authentication Technology*, November 1991.

John Wack, *Establishing a Computer Security Incident Response Capability*, February 1992.

Dennis Branstad, *An Introduction to Secure Telephone Terminals*, March 1992.

Edward Roback, *Disposition of Sensitive Automated Information*, October 1992.

Edward Roback, *Sensitivity of Information*, November 1992.

Shirley Radack, *Guidance on the Legality of Keystroke Monitoring*, March 1993.

Mark Skall and Lynne Rosenthal, *The NIST Graphics Testing Program*, April 1993.

Edward Roback and Barbara Guttman, *Security Issues in Public Access Systems*, May 1993.

John Wack, *Connecting to the Internet: Security Considerations*, July 1993.

Barbara Guttman and Edward Roback, *Security Program Management*, August 1993.

Edward Roback and Barbara Guttman, *People: An Important Asset in Computer Security*, October 1993.

Edward Roback and Barbara Guttman, *Computer Security Policy: Setting the Stage for Success*, January 1994.

Barbara Guttman, Edward Roback, and Elizabeth Lennon, *Threats to Computer Systems: An Overview*, March 1994.

John F. Barkley, *Reducing the Risks of Internet Connection and Use*, May 1994.

Donna Dodson, Edward Roback, and Elizabeth Lennon, *Digital Signature Standard*, November 1994.

Shirley Radack (editor), *The Data Encryption Standard: An Update*, February 1995.

Frederick Boland, *Acquiring and Using Asynchronous Transfer Mode in the Workplace*, March 1995.

Shirley Radack, *Standards for Open Systems: More Flexibility for Federal Users*, May 1995.

Lisa Carnahan, *FIPS 140-1: A Framework for Cryptographic Standards*, August 1995.

Barbara Guttman and Elizabeth Lennon, *Preparing for Contingencies and Disasters*, September 1995.

David Ferraiolo, John Barkley, and Shirley Radack, *An Introduction to Role-Based Access Control*, December 1995.

Robert Bagwill, *Human/Computer Interface Security Issues*, February 1996.

Gary Fisher and Elizabeth Lennon (editor), *Millennium Rollover: The Year 2000 Problem*, March 1996.

Eugene Troy, *Guidance on the Selection of Low Level Assurance Evaluated Products*, April 1996.

Robert Bagwill, *The World Wide Web: Managing Security Risks*, May 1996.

Barbara Guttman, *Information Security Policies for Changing Information Technology Environments*, June 1996.

James Foti, *Implementation Issues for Cryptography*, August 1996.

Barbara Guttman, *Generally Accepted System Security Principles (GSSPs): Guidance on Securing Information Technology (IT) Systems*, October 1996.

Marianne Swanson, *Federal Computer Incident Response Capability (FEDCIRC)*, November 1996.

OTHER NIST PUBLICATIONS

NIST Handbook 148
DATAPLOT Reference Manual, Volume 1: Commands; Volume II: LET Subcommands and Library Functions
By N. Alan Heckert and James J. Filliben

NISTIR 5505
A {xi}-Vector Formulation of Anisotropic Phase-Field Models: 3-D Asymptotics
By A.A. Wheeler and Geoffrey B. McFadden
October 1994 PB95-136628 $19.50

NISTIR 5522
Information Technology Engineering and Measurement Model: Adding lane markings to the information superhighway
By Marvin Zelkowitz and Barbara Cuthill
November 1994 PB95-143145 $19.50

NISTIR 5530
Mapping Integration Definition for Information Modeling (IDEF1X) Model into CASE Data Interchange Format (CDIF) Transfer File
By Igor Simakhodskiy
November 1994 PB95-154670 $25.00

NISTIR 5532
ISDN LAN Bridging
By Tim Boland
November 1994 PB95-154696 $19.50

NISTIR 5538
SGML Parser Validation Procedures
By Ronald B. Wilson
January 1995 PB95-174959 $19.50

NISTIR 5540
Multi-Agency Certification and Accreditation (C&A) Process: A Worked Example
By Ellen Flahavin, Annabelle Lee, and Dawn Wolcott
December 1994 PB95-171955 $21.50

NISTIR 5541
Initial Graphics Exchange Specification (IGES): Procedures for the NIST IGES Validation Test Service
By Jacki A. Schneider and Lynne S. Rosenthal
December 1994 PB95-171427 $19.50

NISTIR 5542
Binary Decision Clustering for Neural Network Based Optical Character Recognition
By Charles L. Wilson, Patrick J. Grother, and C.S.Barnes
December 1994 PB95-171971 $19.50

NISTIR 5546
A Perspective on Software Engineering Standards
By Dolores R. Wallace and Roger J. Martin
December 1994 PB95-171377 $19.50

NISTIR 5557
Lubrication Theory for Reactive Spreading of a Thin Drop
By R.J. Braun, Bruce T. Murray, W.J. Boettinger, and Geoffrey B. McFadden
December 1994 PB95-189460 $19.50

Pub. Number	Title		
NISTIR 5561	*ATM Procurement and Usage Guide*		
	By Tim Boland		
	December 1994	PB95-174967	$19.50
NISTIR 5569	*The MASPAR MP-1 as a Computer Arithmetic Laboratory*		
	By M.A. Anuta, Daniel W. Lozier, and P.R. Turner		
	January 1995	PB95-178893	$21.50
NISTIR 5570	*An Assessment of the DOD Goal Security Architecture (DGSA) for Non-Military Use*		
	By Arthur E. Oldehoeft		
	November 1994	PB95-189510	$19.50
NISTIR 5571	*Operating Principles of MultiKron II Performance Instrumentation for MIMD Computers*		
	By Alan Mink		
	December 1994	PB95-189486	$19.50
NISTIR 5573	*Agile Manufacturing from a Statistical Perspective*		
	By R.G. Easterling		
	October 1995	PB96-109525	$19.50
NISTIR 5576	*Computer Systems Laboratory Annual Report 1994*		
	By Elizabeth Lennon, Shirley Radack, and Ramona Roach		
	February 1995	PB95-209920	$25.00
NISTIR 5589	*A Study on Hazard Analysis in High Integrity Software Standards and Guidelines*		
	By Dolores Wallace		
	January 1995	PB95-198727	$21.50
NISTIR 5590	*Proceedings Report of the International Invitation Workshop on Development Assurance*		
	By Patricia Toth		
	January 1995	PB95-189494	$19.50
NISTIR 5595	*Application Software Interface: ISDN Services for an Open Systems Environment*		
	By Daniel P. Stokesberry		
	February 1995	PB96-131487	$19.50
NISTIR 5596	*Inserting Line Segments into Triangulations and Tetrahedralizations*		
	By Javier Bernal		
	March 1995	PB95-198933	$19.50
NISTIR 5600	*Object-Oriented Technology Research Areas*		
	By Dolores R. Wallace		
	January 1995	PB95-199329	$19.50
NISTIR 5618	*An Expression Formatter for Macsyma*		
	By Bruce R. Miller		
	July 1995	PB95-267829	$19.50

Pub. Number	Title
NISTIR 5623	*An Electronic Implementors' Workshop* By Ted Landberg, Robert Bagwill, and Brenda Gray March 1995 PB95-210936 $19.50
NISTIR 5631	*An Analysis of ANSI ASC X12 and UN/EDIFACT Electronic Data Interchange Standards* By Robert Aronoff and Karen Hsing April 1995 PB95-220554 $19.50
NISTIR 5636	*Persistent Object Base System Testing and Evaluation* By Elizabeth N. Fong April 1995 PB95-220588 $21.50
NISTIR 5641	*Anisotropy of Interfaces in an Ordered Alloy: A Multiple-Order Parameter Model* By R.J. Braun, J.W. Cahn, Geoffrey B. McFadden, and A.A. Wheeler April 1995 PB96-154570 $19.50
NISTIR 5647	*PCASYS — A Pattern-Level Classification Automation System for Fingerprints* By Gerald T. Candela, Patrick J. Grother, Craig I. Watson, R.A. Wilkinson, and Charles L. Wilson August 1995 PB95-267936 $19.50
NISTIR 5652	*Operating Principles of the SBus MultiKron Interface Board* By Alan Mink, George G. Nacht, and John K.Antonishek May 1995 PB95-231783 $19.50
NISTIR 5654	*Defining Environment Integration Requirements* By Barbara Cuthill and Marvin Zelkowitz May 1995 PB96-131545 $19.50
NIST GCR 95-670	*Standards Policy and Information Infrastructure* NIST, Science, Technology and Public Policy Program, Harvard University, and Technology Policy Working Group, Information Infrastructure Task Force May 1995 PB95-231882 $57.00
NISTIR 5657	*An Introduction to the P1003.1g and CPI-C Network Application Programming Interfaces* By Karen Olsen May 1995 PB95-231726 $19.50
NISTIR 5660	*Parallel and Serial Implementations of SLI Arithmetic* By Daniel W. Lozier and P.R. Turner June 1995 PB95-252335 $19.50
NISTIR 5677	*Center for High Integrity Software System Assurance-Initial Goals and Activities* By Dolores Wallace and Marvin Zelkowitz June 1995 PB95-251674 $19.50

Pub. Number	Title
NIST GCR 95-675	*Testability of Object-Oriented Systems* June 1995 PB95-242418 $21.50
NISTIR 5687	*Method and Evaluation of Character Stroke Preservation on Handprint Recognition* By Michael D. Garris July 1995 PB95-251724 $19.50
NISTIR 5691	*Unravel: A CASE Tool to Assist Evaluation of High Integrity Software*, Volume 1 and Volume 2 By James R. Lyle, Dolores R. Wallace, James R. Graham, Keith B. Gallagher, Joseph P. Poole, and David W. Binkley August 1995 PB95-267886 (vol. 1) $21.50 PB95-267894 (vol. 2) $21.50
NISTIR 5695	*Improving Neural Network Performance for Character and Fingerprint Classification by Altering Network Dynamics* By Charles L. Wilson, James L. Blue, and Omid M. Omidvar August 1995 PB95-267803 $19.50
NISTIR 5696	*The Effect of Training Dynamics on Neural Network Performance* By Charles L. Wilson, James L. Blue, and Omid M. Omidvar August 1995 PB95-267845 $19.50
NISTIR 5703	*The NIST ATM Network Simulator — Operation and Programming, Version 1.0* By Nada Golmie, Alfred Koenig, and David Su August 1995 PB96-106851 $21.50
NISTIR 5708	*Electronic Access to Standards on the Information Highway* By Sharon J. Laskowski and Venkata V. Ramayya August 1995 PB96-131578 $19.50
NISTIR 5719	*Mapping Integration Definition for Function Modeling (IDEFO) Model into CASE Data Interchange Format (CDIF) Transfer File* By Igor Simakhodskiy September 1995 PB96-109533 $28.00
NISTIR 5724	*Error-Bounding in Level-Index Computer Arithmetic* By Daniel W. Lozier and P.R. Turner October 1995 PB96-109582 $14.00
NISTIR 5725	*User's Guide for RDA/SQL Validation Tests* (Version 1.0) By Joan Sullivan and Kevin G. Brady December 1996
NISTIR 5726	*Generalized Form Registration Using Structure-Based Techniques* By Michael D. Garris and Patrick J. Grother April 1996 PB96-191374 $19.50

Pub. Number	Title
NISTIR 5735	*Distributed Systems: Survey of Open Management Approaches* By Joseph Hungate and Geraldina Fernandes September 1995 PB96-128202 $19.50
NISTIR 5736	*Comparison of POSIX Open System Environment (OSE) and Open Distributed Processing (ODP) Reference Models* By Geraldina Fernandes and Joseph Hungate November 1995 PB96-131495 $19.50
NISTIR 5737	*A Method to Determine a Basis Set of Paths to Perform Program Testing* By Joseph Poole November 1995 PB96-131503 $19.50
NISTIR 5740	*Virtual Environments for Health Care* By Judi Moline November 1995 PB96-147814 $21.50
NISTIR 5743	*Operating Principles of MultiKron Virtual Counter Performance Instrumentation for MIMD Computers* By Alan Mink November 1995 PB96-131529 $19.50
NISTIR 5757	*Sharing Information Via the Internet - An Infoserver Case Study* By Robert H. Bagwill November 1995 PB96-131511 $19.50
NISTIR 5762	*Standard Generalized Markup Language Test Suite Evaluation Report* By Craig S. Russell November 1995 PB96-154992 $19.50
NISTIR 5769	*C++ in Safety Critical Systems* By David W. Binkley November 1995 PB96-154588 $19.50
NISTIR 5771	*STandard for the Exchange of Product model data (STEP): Procedures for NIST STEP Validation* By Lynne S. Rosenthal November 1995 PB96-154976 $19.50
NISTIR 5788	*Public Key Infrastructure Invitational Workshop September 28, 1995, MITRE Corporation, McLean, Virginia* William E. Burr, Editor November 1995 PB96-166004 $31.00
NISTIR 5789	*Using S-Check Alpha Release 1.0* By Robert Snelick, Nathalie Drouin, and John Antonishek February 1996 PB96-165965 $21.50

Pub. Number	Title
NISTIR 5793	*Data Communications Strategy* By Jerry Mulvenna and Tim Boland January 1996 PB96-167846 $21.50
NISTIR 5799	*Application of the Pointer State Subgraph to Static Program Slicing* By David W. Binkley and James R. Lyle March 1996 PB96-167838 $19.50
NISTIR 5810	*The TMACH Experiment Phase I - Preliminary Developmental Evaluation* Ellen Colvin Flahavin June 1996 PB96-195318 $19.50
NISTIR 5811	*Basic Linear Algebra Operations in SLI Arithmetic* By M.M. Anuta, Daniel W. Lozier, N. Schabanel, and P.R. Turner March 1996 PB96-165931 $19.50
NISTIR 5820	*Distributed Communication Methods and Role-Based Access Control for Use in Health Care Applications* By Joseph Poole, John Barkley, Kevin Brady, Anthony Cincotta, and Wayne Salamon April 1996 PB96-183165 $25.00
NISTIR 5824	*Interoperability Experiments with CORBA and Persistent Object Base Systems* By Elizabeth Fong and Deyuan Yang April 1996 PB96-183140 $21.50
NISTIR 5843	*Component-Based Handprint Segmentation Using Adaptive Writing Style Model* By Michael D. Garris June 1996 PB96-193669 $19.50
NISTIR 5848	*On the Notion of a {xi}-Vector and a Stress Tensor for a General Class of Anisotropic Diffuse Interface Models* By A.A. Wheeler and Geoffrey B. McFadden April 1996 PB96-193776 $19.50
NISTIR 5854	*Computer Systems Laboratory/Computing and Applied Mathematics Laboratory Technical Accomplishments, October 1994 through March 1996* By Elizabeth B. Lennon June 1996 PB96-193768 $21.50
NISTIR 5859	*MV++ v. 1.5A Matrix/Vector Class Reference Guide* By Roldan Pozo June 1996 PB96-195326 $19.50
NISTIR 5860	*IML++ v. 1.2 Iterative Methods Library Reference Guide* By J. Dongarra, A. Lumsdaine, Roldan Pozo, and Karin A. Remington June 1996 PB96-195219 $21.50
NISTIR 5861	*Sparselib++ v. 1.5 Sparse Matrix Class Library Reference Guide* By Roldan Pozo, Karin A. Remington, and A. Lumsdaine June 1996 PB96-193636 $19.50

Pub. Number	Title
NISTIR 5887	*A Diffuse-Interface Description of Fluid Systems* By Daniel M. Anderson and Geoffrey B. McFadden August 1996 PB96-210711 $21.50
NISTIR 5889	*Experimental Models for Software Diagnosis* By Marvin V. Zelkowitz and Dolores R. Wallace August 1996 PB97-113906 $21.50
NISTIR 5894	*Teaching Computers to Read Handprinted Paragraphs* By Michael Garris September 1996
NISTIR 5916	*A Proposed Software Test Service for Special Functions* By Daniel W. Lozier October 1996
NISTIR 5935	*The Matrix Market Exchange Formats: Initial Design* By Ronald F. Boisvert, Roldan Pozo, and Karin A. Remington December 1996

TECHNICAL PAPERS

October 1995 - December 1996

Danner, Bonnie P.; Ippolito, Laura M.; Wallace, Dolores R.; **COMPASS '95 Tenth Annual Conference on Computer Assurance**. NIST Journal of Research, September/October 1995.

Garris, M.D.; Blue, J.L.; Candela, G.T.; Dimmick, D.L.; Geist, J.; Grother, P.J.; Janet, S.A.; Wilson, C.L.; **Off-Line Handwriting Recognition from Forms**. Proceedings of 1995 IEEE International Conference on Systems, Man, and Cybernetics, October 1995.

Lobo, C.; Guthrie, W.F.; Kacker, R.; **A Study of the Reuse of Plastic Concrete Using Extended Set-Retarding Admixtures**. NIST Journal of Research, September/ October 1995.

Radack, S.M.; **Security and the Internet: The Use of Firewalls**. Federation Facts, published by the Federation of Government Information Processing Councils, Fall 1995.

Saltman, R.G.; **Electronic Data Interchange and Small- and Medium-Sized Enterprises**. Internal paper, Fall 1995.

Laskowski, S.J.; Ramayya, V.V.; **Electronic Access to Standards on the Information Highway**. World Standards Day Paper Competition, Fall 1995.

Perine, L.A.; **In Pursuit of an Optimum: A Conceptual Model for Examining Public Sector Policy Support of Interoperability**. Conference on the Interoperability and the Economics of Information Infrastructure, 1995.

Cugini, J.; Dobry, R.; Gligor, V.; Mayfield, T.; **Functional Security Criteria for Distributed Systems**. Proceedings of the 18th National Information Systems Security Conference, October 1995.

Gilbert, D.; **17th National Computer Security Conference, Baltimore, MD October 11-14, 1994**. Proceedings of the 18th National Information Systems Security Conference, October 1995.

Radack, S.M.; **Protecting Information in Systems and Networks: An Update on Cryptography Standards**. Federal Data Center Issues 1995: A View to the Future; Federal 1995 Information Processing Conference.

Harman, D.; **Lab Report Special Section: Natural Language Processing and Information Retrieval Group, Information Access and User Interfaces Division, NIST**. ACM Press SIGIR Forum, Vol. 29, No. 2, pp. 6-10, Fall 1995.

Carnahan, L.J.; **Developing Federal Standards and Accreditations for Data Protection Products**. SPIE/IEEE Photonics East '95 Symposium and SPIE-International Society for Optical Engineering, 1995.

Garris, M.D.; Grother, P.J.; **Generalized Form Registration Using Structure-Based Techniques**. Proceedings of 5th Symposium on Document Analysis and Information Retrieval, 1995.

Wallace, D.R.; Zelkowitz, M.; **Center for High Integrity Software System Assurance**. Proceedings of 2nd IFAC Workshop on Safety and Reliability, Daytona Beach, FL, November 1995.

Sivathanu, U.R.; Hagwood, C.; Simiu, E.; **Exits in Multistable Systems Excited by Coin-Toss Square Wave Dichotomous Noise**. Physical Review E, Vol. 52, pp. 4669-4675, November 1995.

Boisvert, R.; Browne, S.; Dongarra, J.; Grosse, E.; **Digital Software and Data Repositories for Support of Scientific Computing**. Advances in Digital Libraries, Springer-Verlag, New York, NY, pp. 61-72, 1995.

Goldstein, R.E.; Langer, S.A.; **Nonlinear Dynamics of Stiff Polymers**. Physical Review, 1995.

Rushmeier, H.E.; Ward, G.J.; **Lighting, Simulation and Photography: Data, Ideas, and Questions**. Proceedings of Right Light III, 1995.

Fill, J.A.; Dobrow, R.P.; **The Number of m-ary Search Trees on n Keys**. Combinatorics, Probability, and Computing.

Hagwood, R.C.; **Technometrics Book Review of Mathematical Analysis of Spectral Orthogonality by John J. Kalivas and Patrick M. Lang**. Technometrics Book Review, 1995.

Lozier, D.W.; Turner, P.R.; **Parallel and Serial Implementations of SLI Arithmetic**. Theoretical Computer.Science.

Nimeroff, J.; Dorsey, J.; Rushmeier, H.; **A Framework for Global Illumination in Animated Environments**. Proceedings of the 1995 Eurographics Rendering Workshop.

Kacker, R.; Zhang, N.F.; Hagwood, C.; **Real Time Control of Measurement Uncertainty**. Metrologia.

Rushmeier, H.E.; Ward, G.J.; Piatko, C.; Sanders, P.; Rust, B.; **Synthetic Images: Some Ideas About Metrics**. Proceedings of the 1995 Eurographics Rendering Workshop.

Deprit, A.; **L'algebre Symbolique en Mecanique Celeste**. Proceedings of the International Astronomical Union Symposium #172.

Carasso, A.S.; **Error Bounds in Non-Smooth Image Deblurring**. Accepted for publication in SIAM Journal on Mathematical Analysis.

Lozier, D.W.; Turner, P.R.; **Error-Bounding in Level-Index Computer Arithmetic.** Proceedings of the IMACS-GAMM International Symposium on Numerical Methods and Error-Bounds.

Vangel, M.G.; **One-Sided {Beta}-Content Tolerance Limits for Mixed Models with Two Components of Variance**, Error-Bounds Technometrics.

Lozier, D.W.; **Eugene Fiume, An Introduction to Scientific, Symbolic, and Graphical Computation.** Book Review for Mathematics of Computation.

Zhang, N.F.; **Process Capability Index C^dP^ for Stationary Processes**. Journal of Quality Technology.

Braun, R.J.; Cahn, J.W.; McFadden, G.B.; Wheeler, A.A.; **Anisotropy of Interfaces in an Ordered Alloy: A Multiple-Order Parameter Model.** Philosophical Transactions of the Royal Society, Series A.

van Vaerenbergh, S.; Coriell, S.R.; McFadden, G.B.; Murray, B.T.; and Legros, J.C.; **Modification of Morphological Stability Threshold by Soret Diffusion**. Journal of Crystal Growth 147 pp. 207-214, 1995.

Blue, J.L.; Beichl, I.; Sullivan, F.E.; **Faster Monte Carlo Simulations**. Physical Review E, 1995.

Alpert, B.; **High-Order Quadratures for Integral Operators with Singular Kernels.** Journal of Computational and Applied Mathematics 60, pp. 367-378, 1995.

Anderson, D.M.; Worster, M.G.; **Weakly-Nonlinear Analysis of Convection in a Mushy Layer During the Solidification of Binary Alloys.** Journal of Fluid Mechanics 302, pp. 307-331, 1995.

Skeldon, A.C.; McFadden, G.B.; Impey, M.D.; Riley, D.S.; Cliff, K.A.; Wheeler, A.A.; David, S.H.; **On Long-Wave Morphological Instabilities in Directional Solidification.** IMA Journal of Applied Mathematics 6, p. 639, 1995.

Sekerka, R.F.; Coriell, S.R.; McFadden, G.B.; **Stagnant Film Model of the Effect of Natural Convection on the Dendrite Operating State.** Journal of Crystal Growth, 154, p. 370, 1995.

Murray, B.; Wheller, A.; Glicksman, M.E.; **Simulations of Experimentally Observed Dendritic Growth Behavior using a Phase-Field Model.** Journal of Crystal Growth, 154, pp. 386-400, 1995.

Coffey, S.L.; Deprit, A.; Deprit, E.; **Frozen Orbits for Satellites Close to an Earth-Like Planet.** Celestial Mechanics and Dynamical Astronomy, Vol. 59, pp. 37-72.

Vangel, M.G.; Anderson, D.M.; **Richardson's Algorithm and the Approximate Solution of Singular and Inconsistent Matrix Equations.** SIAM Journal on Matrix Analysis and Applications.

Burns, T.J.; Davis, R.W.; Moore, E.F.; **Dynamical Systems Approach to Particle Transport Modeling in Dilute Gas-Particle Flows with Application to a Chemical Vapor Deposition Reactor.** Journal of Computational Physics.

Ferraiolo, D.; Cugini, J.; Kuhn, D.R.; **RBAC: Features and Motivations.** Proceedings of the 11th Annual Computer Security Applications Conference, December 1995.

Barkley, J.F.; **Implementing Role Based Access Control Using Object Technology.** Proceedings of the First ACM Workshop on Role Based Access Control, December 1995.

Ehara, K.; Hagwood, C.R.; Coakley, K.J.; **Novel Method to Classify Aerosol Particles According to Their Mass-to-Charge Ratio — Aerosol Particle Mass Analyzer.** Journal of Aerosol Science, Vol. 27, No. 2, pp. 217-234, 1996.

Wilson, C.L.; Blue, J.L.; Omidvar, O.M.; **Neurodynamics of Learning and Its Effect on Network Performance.** To be published in Journal of Electronic Imaging.

Binkley, D.W.; Lyle, J.R.; **Application of the Pointer State Subgraph to Static Program Slicing.** Submitted to the Journal of Systems and Software.

Mills, Kevin L.; **An Experimental Evaluation of Specification Techniques for Improving Functional Testing.** Journal of Software and Systems, January 1996.

Podio, F.; **Optical Storage Data Integrity.** Imaging and Workflow Conference, National Capitol Chapter of AIIM, February 1996.

Simiu, E.; Heckert, A.; Whalen, T.; **Estimates of Hurricane Wind Speeds By the 'Peak Over Thresholds' Method.** NIST Technical Note 1416, February 1996.

Golmie, Nada; Su, David; **Analysis of the Rate-Based Flow Control Mechanism for Available Bit Rate Traffic in ATM Networks.** Proceedings of the 3rd International Conference on Optical Communications & Networks - OPNET'96, Paris, France, February 27-28, 1996.

Wilson, C.L.; Grother, P.J.; Barnes, C.S.; **Binary Decision Clustering for Neural Network Based OCR.** Pattern Recognition, Vol. 29, Issue 3, pp. 425-437, Pergamon Press, March 1996.

Flahavin, E.C.; **The TMach Experiment Phase I - Preliminary Development and Evaluation.** Submitted to DataPro.

Nielsen, F.H.; **Human Behavior — Another Dimension of Standards-Setting.** ACM StandardView, March 1996.

Saunders, B.V.; **A Boundary Fitted Grid Generation System for Interface Tracking.** Proceedings of the Fifth International Conference on Numerical Grid Generation in Computational Fluid Dynamics and Related Fields, Starkville, MS, March 31-April 5, 1996.

Pozo, R.; **Library Designs for Generic C++ Sparse Matrix Computations of Iterative Methods.** Proceedings of the Copper Mountain Conference on Iterative Methods, April 1996.

Radack, S.M.; Katzke, S.W.; **Role of the Information Technology Laboratory of the National Institute of Standards and Technology in the Development of Standards for Information Technology**. Internal paper, April 1996.

Lyle, J.R.; Wallace, D.R.; **Using a Program Slicing CASE Tool for Evaluating High Integrity Software Systems**. Published on WWW.

Kalisman, A.; McCoy, W.H.; **Video Compression Using a Wavelet Transform for Noisy Channels**. ACM Wireless Networks (special issue), 1996.

Kim, S-Y.; **A Strategy to Support MCS Over Native ATM Service**. Proceedings of the IEEE Southeastcon '96 Conference, Tampa, Florida, April 1996.

Oberndorf, P.A.; Cuthill, B.B.; **Experiences in Environment Integration with Standards**. Proceedings of Software Technology Conference, Salt Lake City, UT, April 1996.

Simiu, E.; Heckert, A.; **Extreme Wind Distribution Tails: A 'Peaks Over Threshold' Approach**. Journal of Structural Engineering, May 1996.

Linn, R.J.; **Using Technology to Manage and Protect Intellectual Property**. Proceedings of IMA/Copyright Office Forum [Journal of IMA], 1996.

Beltracchi, L.; Lyle, J.R.; Wallace, D.R.; **Using a Program Slicing CASE Tool for Evaluating High Integrity Software Systems**. Proceedings of American Nuclear Society Meeting on Nuclear Plant Instrumentation, Penn State University, May 1996.

Gass, S.I.; Witzgall, C.; Harary, H.H.; **Fitting Circles and Spheres to Coordinate Measuring Machine Data**. Proceedings of IFORS Conference, Washington, DC, May 1996. Also submitted to International Journal of Flexible Manufacturing Systems.

Tesoriero, R.; Zelkowitz, M.V.; **Measurement of Process Complexity**. Proceedings of the 7th European Control and Metrics Conference, Wilmslow, UK, May 1996.

Hungate, J.I.; **Standardization Role of the Open system Environment Implementors' Workshop**. Open System Standards Tracking Report, 1996.

Hecht, H.H.; Wallace, D.; **Project Data to Support High Integrity Software Methods**. Published on WWW. Also in Proceedings of American Nuclear Society Meeting on Nuclear Plant Instrumentation, Penn State University, May 1996.

Binkley, D.W.; **Java and C++ in Safety Critical Systems**. Computing Systems, The USENIX Technical Journal, 1996.

Newton, J.; **Application of Metadata Standards**. Proceedings of the 1st IEEE Metadata Conference, May 1996.

Yesha, Y.; **Parameter Replacement for CELP Coded Speech in Land Mobile Radio**. ACM Wireless Networks Journal, 1996.

Saltman, R.G.; **Ready for EDI**. Info Security News, May/June 1996.

Garris, M.D.; Dimmick, D.; **Form Design for High Accuracy Optical Character Recognition**. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 18, No. 6, pp. 653-656, June 1996.

Mills, Kevin L.; **A Knowledge-Based Approach for Automating a Design Method for Concurrent and Real-Time Systems**. Proceedings of the 8th International Conference on Software Engineering and Knowledge Engineering, pp. 529-536, June 10-12, 1996.

Fouquet, Y.A.; Schneeman, R.D.; Cypher, D., Mink, A.; **ATM Performance Measurement: Throughput Bottlenecks and Technical Barriers**. Proceedings of the International Conference on Telecommunication, Distribution, and Parallelism-TDP96, Toulon, France, June 26-28, 1996.

Lyon, G.E.; **Comparing Two Distinct Approaches to Scalability Testing**. Proceedings of the International Conference on Telecommunication, Distribution, and Parallelism-TDP96, Toulon, France, June 26-28, 1996. Also published in Calculateurs Parallels.

Fisher, G.E.; **CSL View of Applications Portability, Scalability, and Interoperability**. ACM StandardView, VOL 4, No. 2, June 1996.

Hagedorn, J.; Blendell, J.; Vaudin, M.; Rushmeier, H.; **A System for Measuring Surface Facet Orientation from Atomic force Microscope Data**. Proceedings of the IEEE Visualization '96 Conference.

Flater, D.W.; **Generalized Message Passing in a Virtual Reality Application**. Journal of Object-Oriented Programming, 1996.

Anuta, M.A.; Lozier, D.W.; Turner, P.R.; **The MasPar MP-1 as a Computer Arithmetic Laboratory**. NIST Journal of Research, Vol. 101, No. 2, pp. 165-174, 1996.

Orlandini, E.; Stella, A.L.; Einstein, T.L.; Tesi, M.C.; Beichl, I.; Sullivan, F.; **Bending Rigidity Driving Transitions and Crumpling Point Scaling of Lattice Vesicles**. Physical Review, 1996.

Anderson, D.; Worster, M.G.; **A New Oscillatory Instability in a Mushy Layer During the Solidification of Binary Alloy**. Journal of Fluid Mechanics 307, pp. 245-267, 1996.

Wakid, S.A.; Radack, S.M.; **The National Institute of Standards and Technology: New Directions in Information Technology**. Open Systems Standards Tracking Report.

Liggett, W.S.; **Measurement for Experimentation**. To be published as book chapter in Statistics for Quality.

Hagwood, C.; Levenson, M.; Sivathanu, Y.; **Computer Intensive Statistics Using Recursive Discrete Probability Functions**. To be published in Journal of the American Statistical Association.

Wheeler, A.; McFadden, G.; Boettinger, W.; **Phase-Field Model of a Eutectic Alloy**. Proceedings of the Royal Society of London, Series A 452, pp. 495-525, 1996.

Liggett, W.S.; Inn, K.G.W.; **Pilot Studies for Improving Sampling Protocols**. To be published in Principles of Environmental Sampling (Second Edition).

Zhang, N.F.; **Statistical Control Charts for Stationary Process Data**. To be published in Technometrics.

Coriell, S.R.; Murray, B.T.; Chernov, A.A.; McFadden, G.B.; **Effects of Shear Flow and Anisotropic Kinetics on the Morphological Stability of a Binary Alloy**. Met. Mater. Trans., 27A, pp. 687-694, 1996.

Warren, J.A.; Murray, B.T.; **Ostwald Ripening and Coalescence of a Binary Alloy in Two Dimensions using a Phase-Field Model**. Modeling and Simulation in Materials Science, 4, pp. 1-15, 1996.

Zhang, N.F.; Postek, M.T.; Larrabee, R.D.; Carroll, L.; Keery, W.J.; **A New Algorithm for the Measurement of Pitch in Metrology Instruments**. Proceedings of SPIE 1996 International Symposium on Microlithography, Santa Clara, CA.

Rust, B.W.; Crosby, F.J.; **Global Temperatures, Gaia, and Fossil Fuel Production**. Submitted to Global Change Biology, 1996.

Holland, M.; Williams, J.; Coakley, K.; Cooper, J.; **Trajectory Simulation of Kinetic Equations for Classical Systems**. Quantum Optics.

Zhang, N.F.; **Autocorrelation Analysis of Some Linear Transfer Function Models and Its Applications in the Dynamic Process Systems**. Journal of the American Statistical Association, 1996.

Rice, J.R.; Boisvert, R.F.; **Summary Report on a Workshop: Scalable Scientific Software Libraries and Problem solving Environments**. IEEE Computational Science and Engineering.

Beichl, I.; Sullivan, R.; **Heaps of Data**. Computational Science and Engineering, 1996.

Boisvert, R.F.; Pozo, R.; Remington, K.R.; Barrett, R.; Dongarra, J.; **Matrix Market: A Web Resource for Test Matrix Collections**. Proceedings of the IFIP Working Conference on the Quality of Numerical Software, Oxford, England, July 8-12, 1996.

Harman, D.K.; **Panel: Building and Using Test Collection**. Proceedings of the 19th Annual International ACM Press SIGIR Conference on Research and Development in Information Retrieval, pp. 335-337, Zurich, Switzerland, August 18-22, 1996.

Anuta, M.M.; Lozier, D.W.; Schabanel, N.; Turner, P.R.; **Basic Linear Algebra Operations in SLI Arithmetic**. Proceedings of the Euro-Par 96, Lyon, France, August 27-29, 1996. [Springer-Verlag Lecture Notes in Computer Science]

Zelkowitz, M.V.; Wallace, D.R.; **Models of Software Experimentation**. Proceedings of the International Conference on Software Engineering Research Network, Sydney, Australia, August 1996.

Levenson, M.S.; **Removing Quantization Noise in Images Using Wavelets**. Proceedings of the 1996 Joint Statistical Meeting, Chicago, IL, August 1996.

Liggett, W.; Moon, K.W.; Handwerker, C.; **An Experimental Method for Refinement of Solderability Measurement**. Circuit World, 1996.

Beichl, I.; Sullivan, F.; **Tree-Lookup for Partial Sums or: How Can I Find This Stuff Quickly?** IEEE Computational Science and Engineering, Vol. 3, No. 1, pp. 13-15, 1996.

Olsen, A.R.; Sedransk, J.; Edwards, D.; Gotway, C.; Liggett, W.; Rathbun, S.; Reckhow, K.; Young, L.; **Statistical Issues for Monitoring Ecological and Natural Resources in the United States**. Environmental Monitoring and Assessment, 1996.

Leigh, S.; Review of the Book **The Pleasures of Probability** by Richard Issac. Technometrics.

Podio, F.L.; **Digital Optical Tape: Technology and Standardization Issues**. Proceedings of the 5th NASA/Goddard Space Flight Center Conference on Mass Storage Systems and Technologies, September 1996.

Wheeler, A.A.; McFadden, G.B.; **On the Notion of a {xi}-Vector and a Stress Tensor for a General Class of Anisotropic Diffuse Interface Models**. Proceedings of the Royal Society of London, Series A.

Lozier, D.; **Software Needs in Special Functions**. Journal of Computational and Applied Mathematics, 1996.

Lawrence, J.; **Nonempty Intersections of Convex Sets**. Discrete and Computational Geometry, 1996.

Wallace, Dolores R.; Ippolito, Laura M.; **Software Verification and Validation**, pp. 22-30 of NIST SP 223, to be reprinted in The Journal of the Quality Assurance Institute, October 1996.

Downey, L.L.; Laskowski, S.J.; Buie, E.A.; Hartson, H.R.; **Symposium Report — Usability Engineering: Industry-Government Collaboration for System Effectiveness and Efficiency**. SIGCHI Bulletin, ACM Press, Vol. 28, No. 4, pp. 66-67, October 1996.

Vrielink, K.H.J.; Baland, E.C.; Devaney, J.E.; **AutoLink: An MPI Library for Sending and Receiving Dynamic Data Structures**. University of Minnesota Super Computer Institute International Conference on Parallel Computing, October 3-4, 1996.

Hogan, M.D.; Radack, S.M.; **The Quest for Information Technology (IT) Standards for the Global Information Infrastructure (GII)**. To be published in the ANSI Reporter.

Abdel-Wahab, H.; Kvande, B.; Nanjangud, S.; Kim, O.; Favreau, J.P.; **Using Java for Multimedia Collaborative Applications**. Proceedings of PROMS 96, October 1996.

Burr, W.E.; Nazario, N.A.; Polk, W.T.; **A Proposed Federal PKI Using X.509 V3 Certificates**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Carnahan, L.; Guttman, B.; **Security Issues for Telecommuting**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Flahavin, E.; Snouffer, S.; **The Certification of the Interim Key Escrow System**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Nazario, N.A.; **Security Policies for the Federal Public Key Infrastructure**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Nazario, N.A.; Burr, W.E.; Polk, W.T.; **Management Model for the Federal Public Key Infrastructure**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Swanson, M.; **U.S. Government-Wide Incident Response Capability**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Wilson, M.; **Marketing and Implementing Computer Security**. Proceedings of the 19th National Information Systems Security Conference, Baltimore, Maryland, October 1996.

Anderson, D.M.; McFadden, G.B.; **A Diffuse-Interface Description of Fluid Systems**. Physics of Fluids.

Beichl, I.; Sullivan, F.; **Making Connections**. IEEE Computational Science and Engineering.

Mitchell, W.F.; **The Full Domain Partition Approach to Distributing Adaptive Grids**. Applied Numerical Mathematics.

Devaney, J.E.; Hagedorn, J.G.; **Transforming a MIMD Hardware Environment into a SIMD Programming Environment**. Proceedings of the 6th Symposium: Frontiers of Massively Parallel Computation, Annapolis, Maryland, October 27-31, 1996.

Fisher, W.M.; **Factors Affecting Recognition Error Rate**. Proceedings of 1996 ARPA Speech Recognition Workshop.

Gallagher, K.B.; **Visual Impact Analysis**. Proceedings of the International Conference on Software Maintenance '96, Monterey, California, November 5-8, 1996.

Cugini, J.; Piatko, C.; Laskowski, S.; **Interactive 3D Visualization for Document Retrieval**. Proceedings of the 5th International Conference on Information and Knowledge Management, Workshop on New Paradigms in Information Visualization and Manipulation, November 16, 1996.

Lipman, R.; Devaney, J.; **WebSubmit - Running Supercomputer Applications via the Web**. Supercomputing 96, Poster Exhibit, Pittsburgh, Pennsylvania, November 17-22, 1996.

Ferraiolo, K.; Ippolito, L.M.; **Conference Report: COMPASS '96, The Eleventh Annual Conference on Computer Assurance**. NIST Journal of Research, November/December 1996.

Willis, J.; Wilsey, P.A.; Peterson, G.D.; Hines, H.; Dashiel, W.H.; **Semi-Automated Validation of VHDL and Related Languages**. Proceedings of VIUF Conference, Fall 1996.

Kuhn, R.D.; **Sources of Failure in the Public Switched Telephone Network**. Accepted for publication in IEEE COMPUTER.

Lozier, D.W.; **A Proposed Software Test Service for Special Functions**. Proceedings of the IFIP Working Conference on the Quality of Numerical Software: Assessment and Enhancement.

Zelkowitz, M.V.; Wallace, D.; **Experimental Models of Computer Research**. COMPUTER, IEEE Computer Society.

Paek, E.G.; **Optical Pattern Recognition Using Microlasers**. Book chapter in Optical Pattern Recognition.

Brady, M.; Rosenthal, L.; **Interactive Conformance Testing for VRML**. Proceedings of the 2nd Annual Symposium on Virtual Reality Modeling Language, 1997.

Ressler, S.; Wang, Q.; Bodarsky, S.; Sheppard, C.; Seidman, G.; **Using VRML to Access Manufacturing Data**. Proceedings of the 2nd Annual Symposium on Virtual Reality Modeling Language, 1997.

Seidman, G.; **Extension Nodes to Facilitate VRML User Interface Development**. Proceedings of the 2nd Annual Symposium on Virtual Reality Modeling Language, 1997.

Wilson, C.L.; Blue, J.L., Omidvar, O.M.; **The Effect of Training Dynamics on Neural Network Performance**. Accepted for publication in Neural Networks, 1997.

Wallace, Dolores R.; Ippolito, Laura M.; **Verifying and Validating Software Requirements Specifications**. Software Requirements Engineering, Second Edition, IEEE Computer Society Press, January 1997.

Garris, M.D.; Omidvar, O.M.; Blue, J.L.; Candela, G.T.; Dimmick, D.L.; Geist, J.; Grother, P.J.; Janet, S.A.; and Wilson, C.L.; **Design of a Handprint Recognition System**. Accepted for publication in the Journal of Electronic Imaging, 1997.

Grother, P.J.; Candela, G.T.; Blue, J.L.; **Fast Implementations of Nearest Neighbor Classifiers**. Accepted for publication in Pattern Recognition, 1997.

Rehm, R.G.; McGrattan, K.B.; Baum, H.R.; Cassel, K.W.; **Transport by Gravity Currents in Building Fires**. Proceedings of the Fifth International Symposium on Fire Safety Science, Melbourne, Australia, March 1997.

Barkley, J.F.; Cincotta, A.V.; Ferraiolo, D.F.; Kuhn, D.R.; **Role Based Access Control in Large Networked Applications**. Proceedings of the High Performance Networks Conference, New York, NY, April 1997.

Conferences, Workshops, Lectures, and Training Courses

In 1996, our organization sponsored, cosponsored, and conducted many conferences, workshops, lectures, and training seminars:

Annual conferences and ongoing workshops

COMPASS, Conference on Computer Assurance
Data Administration Management (DAMA) Symposium
Federal Information Systems Security Educators Association (FISSEA) Conference
Federal Wireless User's Forum (FWUF)
Open System Environment (OSE) Implementors' Workshop (OIW) (now sponsored by the IEEE Computer Society)
National Information Systems Security Conference
North American ISDN Users' Forum (NIUF)
Text Retrieval Conference (TREC)

Specialized conferences and workshops

Army Conference on Applied Statistics
Conference on Leveraging Cyberspace (cosponsored by White House National Economic Council and Xerox PARC)
Electronic Commerce Seminar: Global Marketplace for Small and Medium Enterprises
Export Criteria for Software Key Escrow Encryption
Interoperability and Testing Demonstration of Multimedia Teleconferencing
Invitational Workshop on Computer Vulnerability Data Sharing
Invitational Workshop on Information Technology (IT) Security
Joint Research Conference on Statistics in Quality, Industry, and Technology
Techniques and Tools for Government Information Technology Services
Technologies to Improve Your Software
Training for the Future
Workshop on Cryptographic Applications Program Interfaces
Workshop on Error, Fault, Failure Project
Workshop on Mugshot and Facial Image Standards
Workshop on Quality, Measurement Assurance, and Uncertainty Analysis
Workshop on Role-Based Access Control
Worldwide Electronic Commerce: Law, Policy, Security, and Controls Conference
Symposium on Usability Engineering: Industry-Government Collaboration for System Effectiveness and Efficiency

Lectures

Applied & Computational Mathematics Division Colloquium Series
CAML Laboratory Seminars
Compression Algorithm Group Lecture Series
Digital Video Lecture
High Integrity Systems Lecture Series
High Performance Computing Lecture Series
Information Technology Seminar
Lecture on Optical Pattern Recognition and Neural Nets
Lecture on Supporting Interactive Information Retrieval through Multivariate Anomalies: Computer Security Applications
Relevance Feedback: A Study of End-Users
Research Agenda for User-Centered Collaborative Engineering
Statistical Engineering Division Seminars

Training courses

Analysis of Variance
Arithmetic Operations in Level-Index Arithmetic
Connecting to the Internet Securely
Computer Algebra Course: Maple and Mathematics—Some Examples
Creating an Incident Handling Capability
Distributed Computing & Information Services
Eudora Training
Fortran 90 Programming for Fortran 77 Programmers
Information Systems Security...And You
Introduction to AVS5, AVS/EXPRESS, and IBM Data Explorer
Introduction to C and C++ for Scientists and Engineers
Introduction to Data Compression
Introduction to Error Correction Codes
Introduction to PV-WAVE
Introduction to Visual C++4 and the Microsoft Foundation Class Library
Macintosh Users Group
Programming in Fortran 90
Regression Models
Statistical Design of Experiments
Synchronize Training
Time Series Analysis

ELECTRONIC PRODUCTS AND RESOURCES

For information on ITL electronic products, services, and resources, access the WWW at:

http://www.itl.nist.gov

COMPUTER SECURITY RESOURCE CLEARINGHOUSE

ITL maintains an electronic Computer Security Resource Clearinghouse (CSRC) to encourage the sharing of information on computer security. The CSRC contains computer security awareness and training information, publications, conferences, software tools, as well as, security alerts and prevention measures. The CSRC system, available 24 hours a day, also points to other computer security servers.

Internet Access
To access the clearinghouse via an http client, use the following Uniform Resource Locator (URL):

http://csrc.nist.gov

To connect via gopher and ftp, use the following:

gopher csrc.nist.gov
ftp csrc.nist.gov

To download CSRC files, Internet users can use ftp as follows:

Type ftp csrc.nist.gov
Login to account anonymous, using Internet e-mail address as the password. CSRC files are located in directory pub.

For information on the Cryptographic Module Validation Program:

http://csrc.nist.gov/cryptval/

GUIDE TO AVAILABLE MATHEMATICAL SOFTWARE (GAMS)

http://gams.nist.gov/

NIST GAMS is an electronic resource which provides a cross-index and virtual repository of mathematical and statistical software components of use in computational science and engineering. Using the mathematical software cross index, you can search for software according to:

- □ what problem it solves
- □ package name
- □ module name
- □ text in module abstracts

The Web site provides background information on GAMS, including a project summary, a glossary of terms, repositories indexed, references, credits and disclaimers, and news items. The server also plays host to a variety of other NIST projects related to applied mathematics and statistics.

NORTH AMERICAN INTEGRATED SERVICES DIGITAL NETWORK (ISDN) USERS' FORUM (NIUF)

To access the NIUF Home Page, use the following URL:

http://www.niuf.nist.gov/misc/niuf.html

STANDARD REFERENCE DATABASES

NIST Special Databases

To order NIST Special Databases or NIST Special Software, write or call NIST Standard Reference Data Program, Building 820, Room 113, Gaithersburg, MD 20899, telephone (301) 975-2208; fax (301) 926-0416; e-mail SRDATA@enh.nist.gov

■ Special Database 1 NIST Binary Images of Printed Digits, Alphas, and Text	$ 895
■ Special Database 2 NIST Structured Forms Reference Set of Binary Images (SFRS)	$ 250
■ Special Database 4 NIST 8-Bit Gray Scale Images of Fingerprint Image Groups	$ 250
■ Special Database 6 NIST Structured Forms Reference Set of Binary Images II	$ 250
■ Special Database 8 NIST Machine-Print Database of Gray Scale and Binary Images	$1895
■ Special Database 9 NIST 8-Bit Gray Scale Images of Mated Fingerprint Card Pairs (Volumes 1-5)	$ 750 each
■ Special Database 10 NIST Supplemental Fingerprint Card Data	$ 750
■ Special Database 11 NIST Census Miniform Training Database 1: Binary Images from Microfilm	$1000

■ Special Database 12 NIST Census Miniform Training Database 2: Binary Images from Paper and Microfilm	$1000
■ Special Database 13 NIST Census Miniform Test Database: Binary Images from Paper and Microfilm	$1000
■ Special Database 14 NIST Mated Fingerprint Card Pairs 2	$ 750
■ Special Database 18 NIST Mugshot Identification Database (MID)	$ 750
■ Special Database 19 NIST Handprinted Forms and Characters Database	$ 895
■ Special Database 20 NIST Scientific and Technical Document Database	$1000

NIST Special Software

■ Special Software 1 NIST Scoring Package Release 1.0	$1150

VALIDATED PRODUCTS

The Validated Products List (VPL) lists products that have been validated for conformance to Federal Information Processing Standards (FIPS) for programming languages, database language, computer graphics, operating systems, Open Systems Interconnection, and computer security. It also provides information about NIST's conformance testing programs regarding points of contact, testing procedures, test suites, testing laboratories, and product test reports.

ftp://speckle.ncsl.nist.gov/vpl/intro.htm

For users without access to Web browsers, the programming and database languages product lists are available on the Internet via FTP as follows:

Type: **ftp speckle.ncsl.nist.gov**
Login as user **ftp**
Type your e-mail address preceded by a dash (-) as the password
Type: **cd vpl**
Type: **cd test_files**
Type: **get** followed by the name of the file you want, (e.g., get cobol)

For more information, contact:

Information Technology Laboratory
National Institute of Standards and Technology
Building 225, Room A231
Gaithersburg, MD 20899-0001

Telephone: 301 975-2900

Facsimile: 301 840-1357

Email: itlab@nist.gov

Elizabeth B. Lennon, Writer/Editor

Bessmarie A. Young, Cover Design

Kathie Koenig Simon, Photographer

Don Price, Production

Warren F. Overman, Printing Coordinator

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.