

1998

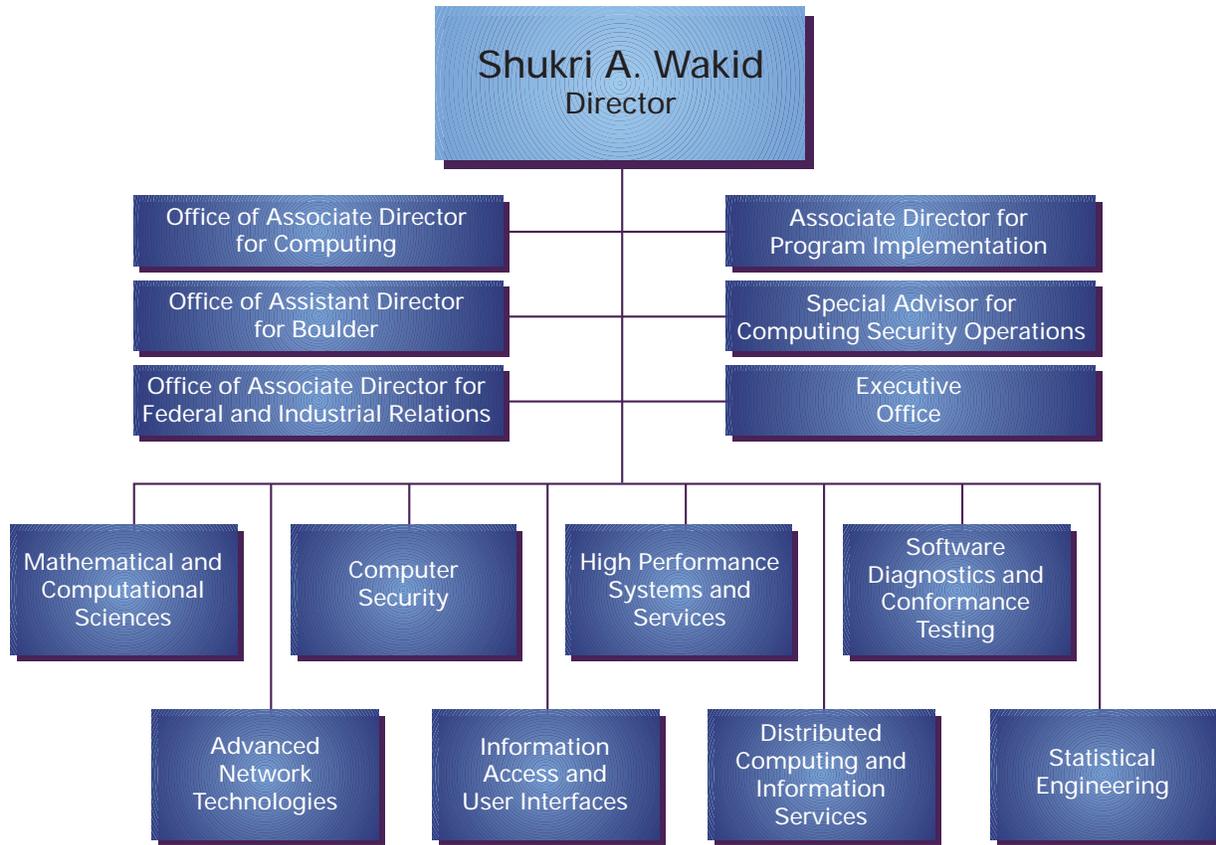
ITL
Technical
Accomplishments

NIST

NISTIR 6254

U.S. DEPARTMENT OF COMMERCE ♦ TECHNOLOGY ADMINISTRATION
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Information Technology Laboratory



NISTIR 6254
October 1998



U.S. DEPARTMENT OF COMMERCE
William M. Daley, Secretary

Technology Administration
Gary R. Bachula
Acting Under Secretary for Technology

National Institute of
Standards and Technology
Raymond G. Kammer, Director

C O N T E N T S

Director's Foreword	1
ITL at a Glance	3
Technical Accomplishments	6
Industry Interactions	30
International Activities	38
Staff Recognition	40
Services to Staff and Public	42



Director's Foreword

September 30, 1998

A significant barrier to the widespread acceptance and use of information technology (IT) services is the lack of standard security technology. The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology has taken the lead in the introduction of the needed standards. ITL's major accomplishment in fiscal year (FY) 1998 was the endorsement by industry and government of the standards that we have championed: the Advanced Encryption Standard (AES), the Public Key Infrastructure (PKI), and the Common Criteria (CC). Commitment to the standards was made at the National Information Systems Security Conference in October 1998 and by various other industry groups.

During the past year, we initiated several new forward-looking major projects in accordance with the ITL project selection criteria, including the following research initiatives:

- Pervasive Computing (Digital Economy). In order to identify measurements and standards needs, ITL launched a major initiative for NIST on this topic and sponsored, jointly with the Defense Advanced Research Projects Agency (DARPA), the first such workshop;
- Biometrics (in cooperation with industry and other government agencies);
- A research center on advanced measurement in cooperation with the University of Maryland (to be open to other universities and organizations); and
- National Information Assurance Partnership (NIAP) (in cooperation with the National Security Agency [NSA] and industry).

ITL achieved major impact in the areas of measurement and standards for a number of its programs. Measurement technology for the Next Generation Internet (NGI) and the introduction of secure protocols for the Internet are creating a seamless, secure environment for millions of Internet users worldwide. In cooperation with NSA through the NIAP, we are ensuring the security of IT systems and networks through cost-effective testing, evaluation, and certification programs. Also noteworthy is our leadership in defining requirements for embedded Java, as well as numerical extensions to this language.

Our impact in the standards arena continues to grow. ITL's leadership in the development of the Advanced Encryption Standard is expected to result in an algorithm that will provide strong security in protecting sensitive unclassified information well into the next century. Our strong industry support on AES, PKI, and CC derives from our outstanding security relationship with industry and NSA. Another success story is our technology transfer of the Role Based Access Control (RBAC) protocol to industry. Working with EDUCAUSE, a consortium of university and industry providers of education material, we participated in the standardization of the Instructional Management System (IMS), which also adopts our RBAC model.

ITL has been successful in FY 1998 in working with NIST scientists to help advance the state of the art in scientific fields using parallel processing. Parallel processing enables the creation of codes that have memory and/or time requirements that cannot be obtained by conventional means. This effort has resulted in standard reference codes and data, theory validation, experiment validation, new analysis tools, new insights, and new parallel algorithms.

Other developments for NIST-wide computer support work include the establishment of a team to design and support a Windows NT enterprise-wide network, implementation of a public key infrastructure for use in authentication and encryption of e-mail, and the design of short Web tutorials for PC users.

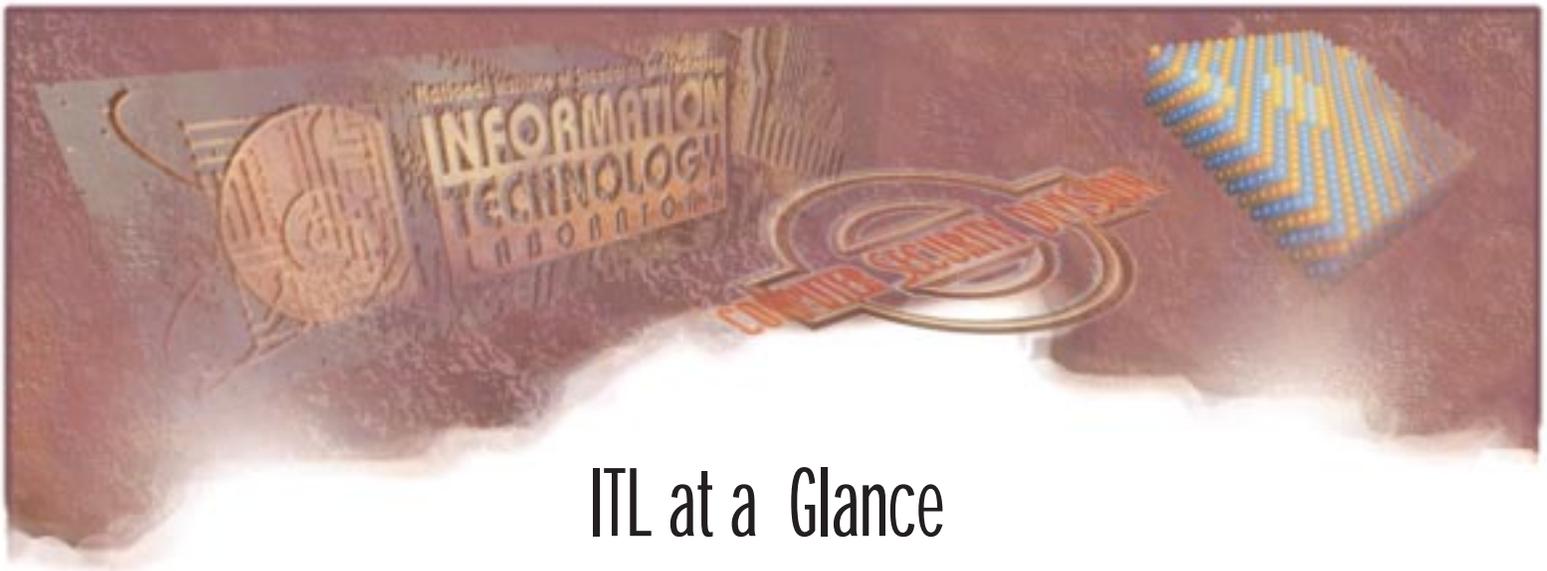
Providing service to industry is another significant ITL contribution. An example is the significantly different digital library version (online) of the Handbook of Mathematical Functions, as well as our Standard Reference Data sets for statistical software.

To balance the additional work while resources are constant, ITL has sunset or transferred to the private sector several successful projects, such as software testing services and test development for several older standards. This allows us to pursue new areas of great potential value to industry where the criticality and uniqueness of our contribution can be felt.

We welcome your interest in the Information Technology Laboratory. In partnership with industry, government, and academia, we will continue to provide the technical leadership for the Nation's measurement and standards infrastructure for information technology, as well as needed IT products and services to promote the U.S. economy in the global marketplace.



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



ITL at a Glance

Shukri Wakid, Director

Paul Domich, Acting Deputy Director

R.J. (Jerry) Linn, Associate Director
for Program Implementation

Fred Johnson, Associate Director
for Computing

David Kahaner, Associate Director
for Federal and Industrial Relations

Paul Domich, Assistant Director
for Boulder

Kathleen Roberts, Acting Senior
Management Advisor

Robert Raybold, Special Advisor
for Computing Security Operations

Ronald Boisvert, Chief of
Mathematical and Computational
Sciences Division

Kevin Mills, Chief of Advanced
Network Technologies Division

Stuart Katzke, Chief of Computer
Security Division

Martin Herman, Chief of Information
Access and User Interfaces Division

Dean Collins, Chief of High
Performance Systems and
Services Division

Oscar Farah, Chief of Distributed
Computing and Information
Services Division

Mark Skall, Chief of Software
Diagnostics and Conformance
Testing Division

Keith Eberhardt, Chief of
Statistical Engineering Division

ITL Mission

Promote the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology.

In support of its mission, ITL provides

- technical leadership and collaborative research in critical infrastructure technologies that promote better development and the use of information technology, and

- high-quality services and supporting infrastructure to help the NIST staff, its collaborators, and its clients address the measurement and standards needs of many industry sectors.

ITL Customers

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

ITL Products and Services

- reference data sets and evaluation software
- proof-of-concept implementations
- tests and test methods
- advanced software tools

- automated software testing techniques
- statistical model-based testing
- specialized databases
- electronic information on the Web
- hardware, software, and network support to NIST staff
- mathematical and statistical consulting services

ITL Resources

- state-of-the-art research facilities in Gaithersburg, Maryland, and Boulder, Colorado

- highly qualified professional and support staff of 452 (includes students), supplemented by 100 guest scientists and faculty members
- operating budget of \$71.8M for fiscal year 1998: \$31.4M from NIST Congressional appropriation (STRS), \$12.3M Consolidated Scientific Computing System (supercomputer), \$0.3M competence funding, \$12.5M NIST Overhead, \$1.8M Advanced Technology Program (ATP), and \$13.5M reimbursable funds, mostly from other federal agencies
- opportunities for cooperative research and interaction with industry and academia

ITL Technical Divisions

- The **Mathematical and Computational Sciences Division** provides technical leadership within NIST in modern analytical and computational methods for solving scientific problems of interest to U.S. industry. The division focuses on the development and analysis of theoretical descriptions of phenomena (mathematical modeling); the design and analysis of the 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 NIST and industry partners.

- The **Advanced Network Technologies Division** enables the development and deployment of next-generation networking technologies for the transmission of multimedia data streams to enable heterogeneous, collaborative computing. The division collaborates as a partner with appropriate industry groups, rather than with specific vendors, in order to foster the widest possible interoperability among products and services within the communications and computer industry. By focusing on enabling technologies, such as protocols, data formats, and algorithms, ITL delivers the widest possible benefit to the industry.

- The **Computer Security Division** provides guidance and technical assistance to government and industry in the protection of unclassified automated information systems. With the growth of electronic commerce and the increased use of distributed systems linked by networks, the need to ensure the security of data and the privacy of information becomes critical.





■ The **Information Access and User Interfaces Division** accelerates 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.

■ The **High Performance Systems and Services Division** enables the effective application of high performance computing and communications systems (HPCC) in support of NIST and its interactions with industry, academia, the federal government, and the public. The division conducts research, development, and evaluation of innovative measurement and test methods, system architectures and software technologies for improved scalability, functionality, flexibility, reliability, and economy of HPCC. It also provides and manages state-of-

the-art facilities that integrate and support an enterprise-wide heterogeneous information technology environment for NIST.

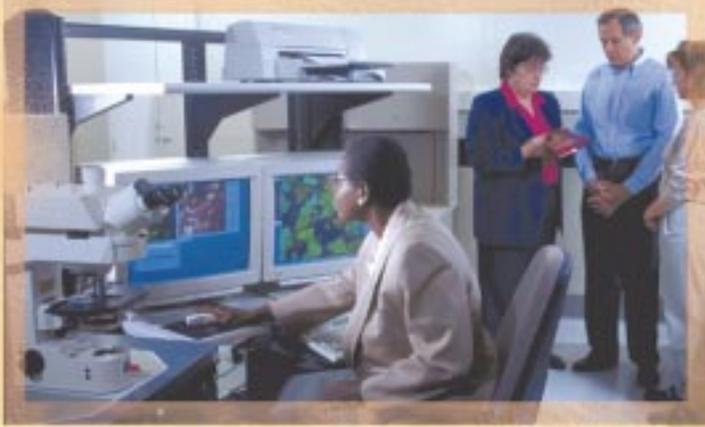
■ The **Distributed Computing and Information Services Division** provides the information technology resources, supporting infrastructure, applied research, and assistance to NIST staff, collaborators, and clients for application in the conduct of scientific, engineering and administrative applications and in the dissemination of information.

■ The **Software Diagnostics and Conformance Testing Division** develops software testing tools and methods that improve quality, conformance to standards, and correctness. The division also participates with industry in the development of forward-looking standards and leads efforts for conformance testing, even at the early development stage of standards.

■ The **Statistical Engineering Division** advances scientific and industrial research by applying statistical methods to the collection and analysis of data critical to NIST scientists and collaborative partners in industry. The division provides expertise in the development of statistical modeling and analysis methods relevant to measurement science and technology. By developing strong collaborative research relationships with the NIST scientific and technical staff, statisticians in the division bring state-of-the-art statistical tools and techniques to NIST research and development programs. ■

Descriptions of selected ITL technical accomplishments appear in the following section. Numbers after photo captions tie the photos to the related project description.

Mathematical and Computational Sciences Division Projects



F. Hunt inspects a scanning electron microscope (SEM) image of the microstructure of a metallic paint used in automobile coatings. M. McKnight (BFRL), T. Vorburger (MEL), and M. Nadal (PL) discuss a piece of an automobile from which the SEM sample was taken. The project combines optical and microstructural measurements as part of a multi-laboratory effort to develop measurement sciences for optical reflectance and scattering. (1)

Measurement Science for Optical Reflectance and Scattering (1)

This NIST competency program resulted from a mathematical modeling collaboration with NIST's Building and Fire Research Laboratory. An ITL researcher developed the idea of using ITL computer graphics expertise to bear on the problem of characterizing and evaluating the appearance of surfaces. The goal is to produce photo-realistic rendered images of objects when given physical measurements and surface specifications. The project will generate a NIST-based measurement database for use by the computer graphics industry and other industries concerned with the appearance of coated surfaces. Our High Performance Systems and Services Division provides computer graphics support for the project. In FY 1998, we developed research plans for the project and established collaborations with industry and academia.

NIST Guide to Available Mathematical Software (GAMS) (2)

A primary tool for the dissemination of information about mathematical

software tools, GAMS indexes more than 10,000 software components from 110 libraries and packages. These components, updated in FY 1998, were either developed at NIST, selected for use at NIST, or archived at netlib, an external repository of the numerical analysis community. This year we also evaluated alternative database systems. GAMS is accessed by 10,000 external users each month. The Web site is <http://math.nist.gov/gams/>.

MPEG and Image Compression Tools (3)

To respond to industry's need for image fidelity metrics, ITL is developing tools, image fidelity metrics, and standard reference materials to facilitate the verification of MPEG2 extensions. We performed research on image modeling and metrics with spin-offs on edge detection. In FY 1998, we worked with the Society of Motion Picture and Television Engineers (SMPTE) committee to modify existing software and develop new software to provide tools and reference material. We also collected and developed reference material for testing still image compression algorithms against common compression artifacts.



R. Boisvert, M. McClain, and B. Miller plan improvements to the Guide to Available Mathematical Software (GAMS), a cross-index and virtual repository of software components for computational science and engineering developed by ITL. (2)



R. Onyschczak, O. Kia, and A. Schaff compare subjective rankings of visually degraded pictures and the scores assigned by a variety of image fidelity metrics, including NIST-developed alternatives designed to be better suited to human perception systems. (3)

NIST Sparse BLAS (4)

In a project which complements and adds value to the Matrix Market, ITL continues to work with the BLAS Technical Forum to establish community consensus on an interface to kernel operations for sparse linear algebra. The forum is an industry/government/academic working group with participants from SGI/Cray, NEC, Intel, the Numerical Algorithms Group, Ltd., Lucent Technologies, HP/Convex, Tera Computers, Texas Instruments, Visual Numerics, and IBM. In FY 1998, we revised and updated the interface specifications issued last year and developed reference implementations. The project Web site is <http://math.nist.gov/spblas/>.

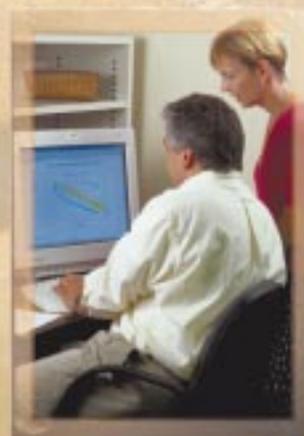
Micromagnetic Modeling (5)

In response to industry's need for reference software and standardized test cases to test modeling software, ITL collaborated with NIST's Materials Science and Engineering Laboratory to develop reference, open source code computational tools for the micromagnetic modeling of materials. Accurate micromagnetic modeling is critical for the design and development of magnetic devices such

as recording heads, field sensors and magnetic nonvolatile memory. Following an alpha release of the micromagnetic package with the 2D solver in January 1998, we incorporated feedback from industrial and academic users into subsequent alpha releases and the design in process of the 3D solver. In September 1998, we publicly released the micromagnetic package with the 2D solver. The micromagnetic software and documentation are available at <http://math.nist.gov/oommf/>.

Digital Library of Mathematical Functions (DLMF)

ITL is creating an interactive, Web-based Digital Library of Mathematical Functions which will replace the NBS Handbook of Mathematical Functions, Applied Mathematics Series 55, published in 1964. Known as AMS 55, this classic reference work contains formulas, graphs, and tables that characterize the higher functions of applied mathematics. In FY 1998, project participants developed an outline of the technical material to be collected, assembled a board of associate editors, and sought funding



R. Pozo and K. Remington check the performance of the NIST Sparse BLAS Library, the reference implementation of an emerging standard for basic operations on sparse matrices developed by ITL. (4)

Images used by ITL researchers for comparing image fidelity metrics. (3)

for the project. A Web site that functions as a working prototype was established:

<http://math.nist.gov/DigitalMathLib/>.

Object Oriented Finite Element Software for Materials Science (OOF)

In collaboration with NIST's Materials Science and Engineering Laboratory, ITL is developing software that can read a micrograph, assign microscopic materials' properties to features in the image, perform virtual experiments to determine the macroscopic properties of the material, and extract useful results. The software will be usable by researchers with no experience in programming or finite element methods and should be easily modifiable to handle new types of materials. The first working versions of PPM2OOF (for assigning properties to images) and OOF (for performing virtual experiments) were released in 1996. This year we added new features, issued the first version of the OOF manual, and completed OOF and PPM2OOF version 1.0.

The Web site is

<http://www.ctcms.nist.gov/~wcraig/oof/>.

Java Numerics

ITL's Java Numerics project seeks to support community efforts to improve the Java language and environment for scientific computing by assessing Java's potential for scientific computations and developing community-supported standardized class libraries for core mathematical computation. Two ITL mathematicians co-chair the Numerics Working Group of the Java Grande Forum (JGF), an open forum of industrial, government and academic researchers, and software developers interested in improving the Java language and environment for use in high performance computing. ITL staff are working with The MathWorks Inc. on a model public class library for matrix computations. See <http://math.nist.gov/javanumerics>.

The Matrix Market

ITL's Matrix Market provides algorithm and software developers with convenient access to standard, industrial-strength test problems in order to evaluate the performance of sparse matrix algorithms on realistic problems, as well as to form a basis

for comparison among emerging software packages. In FY 1998, the division improved the presentation of matrix statistics, developed new submission standards with the Boeing Company and Rutherford Appleton Laboratories (UK), and incorporated a new collection of test problems in cooperation with industry. Visit the Web site at

<http://math.nist.gov/MatrixMarket/>.

Fortran 90 Bindings for OpenGL

The purpose of this ITL project is to specify complete Fortran 90 bindings for OpenGL and to develop a portable reference implementation for the bindings. We worked with the OpenGL Architecture Review Board (ARB) to get the Fortran 90 bindings adopted as the official Fortran API for OpenGL. Following the recommendations of J3, the bindings were revised and approved by the OpenGL ARB and implemented as f90gl Version 1.1. In FY 1998, we also completed the revised reference implementation. The Web site is

<http://math.nist.gov/f90gl/>. ■

ITL's D. Porter and M. Donahue, who are developing a public code for micromagnetic modeling, confer with R. McMichael of MSEL on experimental verification. (5)





V. Schaal and M.Ranganathan work on a distributed system that enables the capture and subsequent live playback of user activity in a multi-user collaborative application. (6)

Advanced Network Technologies Division Projects

Mobile Streams (6)

With design input from the University of California at Santa Barbara and the University of Maryland at College Park, ITL is designing and building application middleware; scripting globally distributed, reconfigurable, event-driven applications; and investigating the infrastructural needs for such applications. We developed a preliminary prototype of our system, demonstrated its capabilities, and developed a small application suite. This experience led to significant changes in our design and approach.

IPsec and IPv6 Technologies (7)

This ITL project aims to expedite the research, development, standardization and commercialization of next-generation Internet security and IPv6 technology. The project delivers rapid prototypes and testing technology that are used widely by IPsec and IPv6 researchers and developers. In FY 1998, we released NIST Cerberus version 0.1 and announced NIST IPsec-WIT and NIST IPsec-WIT+IKE. We also conducted research and development

of the IKE key management prototype. We collaborated with the Computer Security Division in this effort. Web sites are <http://www.antd.nist.gov/itg/cerberus/> and <http://ipsec-wit.antd.nist.gov/>.

Hybrid Fiber-Coaxial (HFC) Network (8)

At the request of the IEEE 802.14 Working Group, ITL serves as an unbiased third party to evaluate Medium Access Control (MAC) proposals being considered for a CATV data modem using existing fiber-coaxial network to homes. Our performance evaluation on 18 different technical proposals assisted in the convergence towards a single MAC solution. The Web site is <http://www.hsnt.nist.gov/>.

IP Quality of Service (QoS) (9)

In this project, ITL researches and develops test methods and tools that enable the design and engineering of QoS-sensitive applications over today's Internet technology. The project also aims to expedite the design, standardization, and

commercial implementation of new IP QoS technologies and to deliver testing technology for use by IP QoS researchers and developers. In FY 1998, we released the initial prototype of an Integrated Services Protocol Instrument (ISPI). ISPI is an interactive, integrated tool for measuring the performance of QoS-sensitive data streams. We also developed the prototype of NIST Net, a general-purpose tool for emulating performance dynamics in IP networks. Web sites are <http://www.antd.nist.gov/itg/ispi/local/ispi-users.html> and <http://www.antd.nist.gov/itg/nistnet/local/nistnet-users.html>.

Digital Video Over ATM (10)

This project seeks to improve quality and promote interoperability across digital video applications and services. In FY 1998, we worked with Bellcore researchers and Bell Atlantic engineers on Video-on-Demand (VoD) quality tests. A VoD system, based on the Digital Audio Visual Council (DAVIC) Specifications V.1.1, was built jointly by NIST and Korea Telecom. ITL researchers and visiting scientists contributed to test specifi-



S. Shah, H. Fang, K. Glenn, and S. Frankel work on the development of test and measurement tools for Next Generation Internet technologies including IP QoS, IPv6, and Internet security protocols. (7)

cations for DAVIC. We worked with the ISO/IEC JTC1 to develop the Digital Storage Media Command and Control (DSM-CC) Conformance Standard, part 10 of the ISO/IEC 13818 Moving Picture Experts Group (MPEG) 2 standard. We enhanced the VoD testbed system and we developed a source traffic model for variable bit rate MPEG2 video, which was incorporated into the NIST ATM/HFC Network Simulator.

All-Optical Transport Networks with Wave Division Multiplexing

Wave Division Multiplexing (WDM) is emerging as a promising optical network technology to meet the challenge of high-bandwidth demand. With WDM, an optical fiber is engineered to carry multiple wavelengths, each with a capacity ranging into the tens of Gigabits/sec. ITL provides leadership in areas, such as standards development, that will facilitate a rapid commercialization and deployment of all optical networks. We are also developing WDM performance modeling and testing tools critical to the communication industry. In FY 1998, we initiated collaborative arrangements with major WDM component vendors, local exchange carriers, and Internet service providers to build a WDM testbed for interoperability testing, survivability testing, and performance measurement. We also worked with members of standards

groups and industry consortia such as the ANSI Committee T1 and the Optical Interworking Forum.

ATM (Asynchronous Transfer Mode) Network Testing

ITL initiated this project to help meet industry demands for sound and effective ATM network protocol standards that lead to interoperable ATM products. In FY 1998, we used the NIST ATM/HFC Network Simulator to assess ATM traffic management algorithms. This year we completed the ATM call signaling conformance test suite. We continued work on conformance and interoperability tests and specifications for several ATM protocols.

We completed Extended Finite State Machine (EFSM) modeling of all Private Network-Network Interface (PNNI) protocols using Promela & SPIN tools. We worked closely with Bell Labs to develop formal models for generation of PNNI test cases. Performance evaluation was done through direct measurement on a live testbed and through simulation using a PNNI simulation tool. Finally, we



ITL researchers Y. Saintillan, N. Golmie, and F. Lapeyrere evaluate the performance of HFC network protocols using the NIST ATM/HFC Network Simulator. (8)

developed a tool set for implementation of the Available Bit Rate (ABR) test suite and released a new ATM/HFC Network Simulator incorporating most of the ATM ABR service flow control alternatives.

DARPA Intelligent Collaboration and Visualization (IC&V)

In this joint project with the Information Access and User Interfaces Division, we developed methods and software tools to support the evaluation of collaborative systems. We developed a reconfigurable, distributed scripting system, and then used this system to record and replay user events from a Java-based collaborative tool. The record and replay facility enables repeatable generation of user events. We also developed a tool for emulating routing packet loss and congestion that can be used for protocol evaluation. Partners in this work include the MITRE Corporation, the National Imagery and Mapping Agency (NIMA), and Carnegie Mellon University (CMU).

Java-Based Multimedia Collaboration

Working with the University of Old Dominion and UNC Chapel Hill, ITL designed and implemented an adaptable and extensible architecture, called Java Collaborative Environment (JCE). JCE enables platform-independent multimedia conferencing and collaborative application sharing. We completed and released the beta version of JCE, including libraries and utilities providing collaborative mechanisms for application sharing, conference and floor control management, replication management, both socket and RMI-based network communications, and audio. In FY 1998, we completed the development and implementation of a Java-based video tool and we integrated it with the JCE, including development of video window management and synchronization of inter-streams. This project is now completed.

Next Generation Internet (NGI)

As part of the NGI Initiative, ITL focused on advanced network technologies in FY 1998 including

Internet protocol version 6 (IPv6) with the Computer Security Division and RTP, RSVP, and Quality of Service (QoS) in packet switched networks. Experimenting with new technologies, we developed a Real Time Protocol / Resource Reservation Protocol (RTP/RSVP) testbed, instrumentation, and tools for QoS. We produced a protocol simulation and analysis for advanced ATM networks. We developed criteria, tests, and test methods for Internet security, cryptographic technology, and advanced authentication technology. We worked on public key and key management infrastructure, and IPv6 with integrated security and remotely accessible interoperability testbed. We also demonstrated new applications for manufacturing by developing and demonstrating Internet access to a wide range of measurement and calibration services.

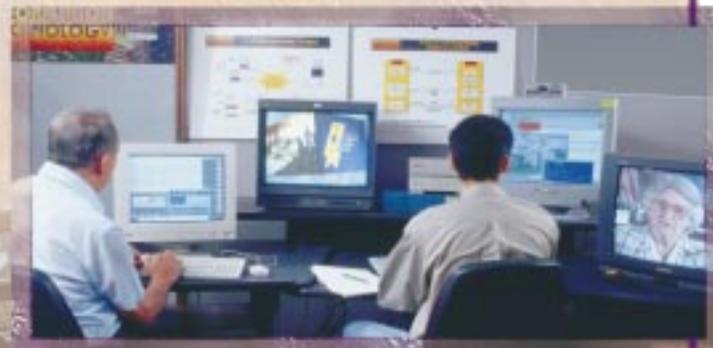
Streaming Synchronized Multimedia

This ITL project facilitates the development of interoperable, industry consensus standards

for the network multimedia and the Web. We work closely with the SMIL (Synchronized Multimedia Integration Language) specification of the Synchronized Multimedia working group of the World Wide Web Consortium (W3C). SMIL Version 1.0 was approved in June 1998. In FY 1998, we assisted the working group in creating a dynamic, but secure, Web page to register all vendors' SMIL player feature lists. We also hosted the SMIL interoperability test on February 12-13, 1998. We provided test scenarios, logistics, and facility support. In June 1998, we completed the first version of a Java-based SMIL player, which operates with Java-enabled browsers to stream synchronized multimedia objects over the network. This player has been used extensively during interoperability experiments with other vendors, e.g., RealNetworks. ■

A. Koenig and K. Zamani test MPEG1 and MPEG2 audio-visual encoding/decoding with a DAVIC-based Video on Demand system developed at NIST. (10)

Michael Zink, a guest researcher, configures a testbed of NIST Switch prototypes. (9)



NIST Net allows controlled, reproducible experiments with QoS sensitive Internet applications and protocols to study the effect of Internet performance dynamics on adaptive video applications. (9)

Computer Security Division Projects

Advanced Encryption Standard (AES) (11)

ITL initiated the development of the AES to find an eventual successor to Federal Information Processing Standard (FIPS) 46-2, Data Encryption Standard (DES). In FY 1998, we announced the candidate algorithms for public review in August 1998. Comments are being solicited from industry, academia, standards bodies, and the public through next spring. We will use comments received in this process to narrow the field of candidate algorithms to five or fewer for a second round of public evaluation. When the AES is selected, we expect that the algorithm will provide strong security in protecting sensitive unclassified information well

into the next century. The Web site is <http://csrc.nist.gov/encryption>.

National Information Assurance Partnership (NIAP) (12)

In October 1997, ITL and the National Computer Security Center of the National Security Agency (NSA) formed NIAP, a partnership for testing methods and measures to ensure the quality of information security systems. In FY 1998, working as a member of the Common Criteria Implementation Board, ITL submitted the Common Criteria for Information Technology Security Evaluation (CC), Version 2.0, specifications to the International Organization for Standardization (ISO) where it is now in the balloting process for acceptance as an International Standard. We also participated in the development of evaluation methodology for testing against the CC. We contributed to two draft documents on the CC scheme and laboratory accreditation of testing laboratories through the

National Voluntary Laboratory Accreditation Program (NVLAP), and we sponsored a public workshop on the NIAP Common Criteria Evaluation and Validation Scheme for IT Security in September 1998. Finally, we facilitated the development of a protection profile containing functional and assurance requirements for implementing Role Based Access Control features in software products, a commercial Operating System (CS2) protection profile that gives a baseline set of security requirements for commercial, off-the-shelf IT, and a protection profile for telecommunication switches. The Web site is <http://niap.nist.gov>.

Public Key Infrastructure (PKI) (13)

Secure, interoperable PKI technology supports security services such as confidentiality and digital signatures required in electronic business transactions. In collaboration with industry partners and other federal agencies, ITL is working on further standardizing public key cryptography by establishing a federal PKI consisting of a network of Certificate Authorities (CAs). In FY 1998, we developed an initial implementation of a root CA and related testbed for the federal PKI. With industry we initiated the development of a set of security requirements and tests for PKI. We enhanced the Minimum Interoperability Specification for PKI Components (MISPC) to include support for confidentiality. ITL chairs the Technical Working Group (TWG) of the Federal PKI Steering

J. Foti, M. Smid, and E. Roback analyze the cryptographic algorithms under consideration for the Advanced Encryption Standard (AES). (11)



Committee, which includes technology representatives from federal agencies and industry. PKI CRADA partners include AT&T Corporation, CertCo, Certicom Corporation, Cylink Corporation, Digital Signature Trust Company, DynCorp Information & Engineering Technology Inc., Entrust Technologies, Inc., Frontier Technologies Corporation, GTE, ID Certify, MasterCard International, Microsoft Corporation, Motorola Inc., SPYRUS Inc., VeriSign Inc., and Visa International. The Web site is <http://csrc.nist.gov/pki/>.

Computer Security Resource Clearinghouse (CSRC)

ITL's CSRC Web site provides access to crisis response information as well as information on security-related threats, vulnerabilities, and solutions. CSRC represents ITL's work in developing, prototyping, testing, and implementing computer security standards and procedures to increase security measures and to create more robust security architectures. In FY 1998, we completely restructured the CSRC. The site is now easy to navigate by the addition of a topic bar that appears on each page. A search engine has been added to aid in locating files. The CSRC is widely acknowledged throughout the federal government as a primary information source. More than half of the accesses to the Web site come from non-government sources in the academic and private sectors. The Web site is <http://csrc.nist.gov>.

Cryptographic Module Validation Program (CMVP)

In FY 1998, ITL's Cryptographic Module Validation Program validated 19 modules as conforming to Federal Information Processing Standard (FIPS) 140-1, Security Requirements for Cryptographic Modules. FIPS 140-1 specifies four separate levels of security provided by Cryptographic Modules, with each level providing increased security and assurance. The total number of validated modules as of September 30, 1998, is 29, giving federal agencies a variety of cryptographic products, both hardware and software, available for use in securing sensitive information. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. ITL's Computer Security Division and CSE serve as the validation authorities for the program. The Web site is <http://csrc.nist.gov/cryptval>.



S. Katzke and his NSA counterpart, L. Giles, review technical details of the proposed security evaluation program workshop that will include 200 information technology (IT) product developers, prospective security testing laboratories, and consumers of IT security products from the U.S., Europe, and Asia. (12)

Encryption Key Recovery

To meet Administration objectives of providing key recovery capability in federal government systems, ITL continues to support the technical advisory committee established by Presidential directive in 1997 for the development of a federal standard for encryption key recovery. NIST participates as a federal liaison on the committee and serves as its Executive Secretary. In FY 1998, the committee developed a working draft of the standard, including a proposed key recovery model, as well as proposed key recovery functions and associated security and assurance requirements.

We participated extensively in developing the key recovery model and reviewing the draft technical recommendations. The Web site is <http://csrc.nist.gov/tacdfipsfkmi/>.

Federal Computer Incident Response Capability (FedCIRC)

For the past several years, ITL administered FedCIRC which provided a service to federal agencies to handle computer incidents, develop standards and guidelines, train federal computer users, and gather vulnerability data for the purpose of increasing computer security and reliability. In FY 1998, we managed the program and provided guidance to federal agencies through presentations, sample policies, and documents. We standardized the methods for reporting incidents, collecting information, and distributing vulnerability-related data and statistics. Finally, we prepared for the transition of the project to the General Services Administration on October 1, 1998.

GITS Information Technology (IT) Security Training

Funded by the Government Information Technology Services (GITS) Board, this pilot project establishes a single focal point for the development of IT security training for use throughout the federal government. The project focuses on executive and senior management attention on the critical need to

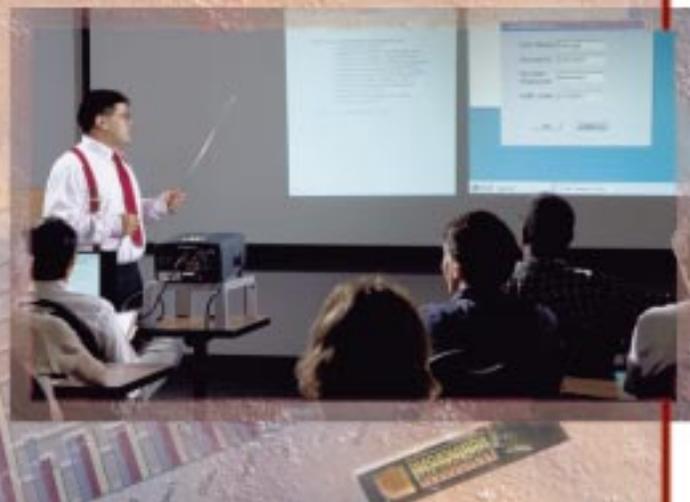
provide appropriate IT security training to their staff. The objectives of the project are to promote the need for IT security training throughout the government; to coordinate the dissemination of existing laws, policies, procedures, and training materials; and to assist in the development of a repository of IT security training resources appropriate for use by federal agencies. In FY 1998, we initiated the project, established a proof-of-concept Web site that contains a sample set of training materials, and organized a work group within the Federal Information Systems Security Educators' Association (FISSEA) to solicit materials for the repository. The Web site is <http://csrc.nist.gov/gits>.

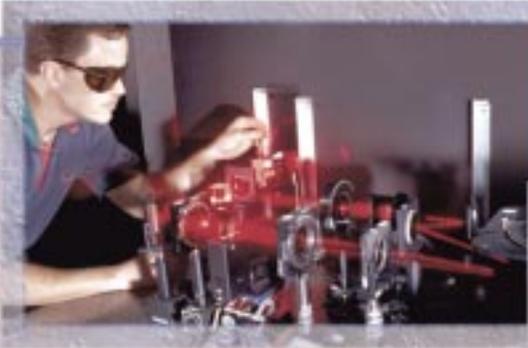
Role Based Access Control (RBAC)

Role based access control is an alternative access control model that is attracting increasing attention, particularly for commercial applications. ITL developed the first formal, general model for RBAC, a new concept which provides access to IT resources

based on a user's role in an organization. With RBAC, security is managed at a level that corresponds closely to an organization's actual business structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. To promote the transfer of RBAC to industry and government, ITL developed application program interfaces (APIs), administrative tools, and prototype systems and demonstrations including an RBAC implementation in an intranet environment. ITL's Ramaswamy Chandramouli and Ravi Sandhu, George Mason University, received the 1998 National Information Systems Security Conference (NISSC) Best Paper Award for a paper entitled "Role Based Access Control Features in Commercial Database Management Systems." Our Software Diagnostics and Conformance Testing Division also works on RBAC projects. The Web site is <http://hissa.ncsl.nist.gov/rbac/>. ■

Demonstration by N. Hastings of an automated software testing tool used to test Public Key Infrastructure applications. (13)





C. Watson shows the Optical Pattern Recognition System working using fingerprints. (14)

P. Hsiao and C. Sheppard discuss ITL software tools developed to evaluate the usability of the Web. (15)



Information Access and User Interfaces Division

Optical Information Processing (14)

One of the major barriers to the commercial application of optical technology to information processing is the high cost of system development and manufacture. The development of better system-level metrology is needed to allow more computer-based methods to be used in this process. As a test case, we designed an optical pattern recognition system to be performed on an input image (at video rates) versus a large reference set, for example, 1000 faces with images of 640 by 480 pixels or larger. We constructed both an optical pattern recognition system and a holographic memory system that we have instrumented and used to address the metrological needs of these applications. In FY 1998, we developed an accurate simulation of an optical system and produced a real-time video fingerprint test data CD. Researchers and developers of systems which use optical pattern classification are benefiting from ITL's work.

Usability Engineering (15)

The success or failure of software products and Web sites often hinges

as much on ease of use as on pure functionality. ITL develops methods and metrics to assist designers and authors build in usability as an intrinsic part of their products. In FY 1998, we sponsored two Industry Usability Workshops that introduced the notion of usability into the procurement decisions of industries who regularly purchase commercial, off-the-shelf (COTS) software. We also established the Usability Engineering for Government Systems Symposium, now in its 3rd year. Finally, we developed the WebMetrics toolset that contains rapid, remote, and automated tools to help in producing usable Web sites: <http://www.nist.gov/webmetrics>.

Human Language Technology - Spoken Language Technologies (16)

Funded by the Defense Advanced Research Projects Agency and the National Security Agency, ITL continues to advance the state of the art in spoken language technologies by focusing its benchmark tests on ever-more-difficult domains such as the recognition of broadcast news recordings in several languages. Since the early 1980s, we developed test protocols, speech corpora, and

software tools for the evaluation of several spoken language technologies and implemented benchmark tests of these technologies.

In FY 1998, we conducted spoken document retrieval and multilingual broadcast news tests and developed initial supplemental speech recognition metrics (i.e., Information Extraction and Topic Detection and Tracking). Numerous industries benefit from improvements in automatic speech recognition technologies including telecommunications, information technology, financial services, and security. ITL's spoken language software tools are available at: <http://www.nist.gov/speech/software.htm>.

Text REtrieval Conference (TREC) (17)

Initiated in 1992, the TREC conference series focuses on the creation, administration, and analysis of large, complex data collections. Each TREC conference had more participants than the year before, with a total of 51 groups (including representatives from 12 different countries and 21 companies) submitting retrieval results in TREC-6, held in FY 1998. The number of different retrieval sub-problems that

have been explored also increased each year, starting with two main tasks in TREC-1 and increasing to ten tasks in TREC-6. The additional tasks and test collections extended the focus of TREC to include such areas as retrieval in languages other than English, retrieval of spoken documents (i.e., recordings of speech), and searching over larger collection sizes (20 gigabytes of documents rather than two). This year we also developed metrics to measure intra-topic variation within a data set. The Web site is <http://trec.nist.gov>.

Visualization for Access to Complex Documents (18)

ITL is demonstrating that three-dimensional visualization can be a valuable interactive medium between the user and a retrieved set of documents. ITL personnel conceived and developed the various NIST Information Retrieval Visualization Engine (NIRVE) prototypes, including basic visualization design, together with various implementation issues

J. Garofolo and B. Lund explain how Automatic Speech Recognition and Spoken Document Retrieval technologies work to Adam Neely, 5th grade student. (16)



(e.g., integrating software using OpenGL, Tcl/Tk, Xlib, and Netscape). Under contract to ITL, the Psychology Department of the Catholic University of America (CUA) is developing, executing, and analyzing user tests for the NIRVE prototype in order to evaluate the strengths and weaknesses of various approaches (3D, 2D, text) to information visualization. In FY 1998, we developed a new version for CUA testing with global metaphor for clusters, document titles in docfield, and keyword concept mapping legend. The Web site is <http://zing.ncsl.nist.gov/~cugini/uicd/sphere-slide-00.html>.

Visualization and Virtual Reality for Manufacturing and the VRML Anthrokids Application (19)

ITL and NIST's Manufacturing Engineering Laboratory are working together to apply advanced information technology to manufacturing applications. When the Consumer Product Safety Commission (CPSC) sought help with their data access problems, we began a related effort to digitize and visualize child anthropometric data

E. Voorhees confers with the TREC "assessors." The role of human judgments in creating viable benchmark tests for text retrieval is critical. (17)



so that it is more readily available to manufacturers. Using the Virtual Reality Modeling Language (VRML), we created a number of prototype systems that were "firsts." In FY 1998, we integrated the Knowledge Revolution dynamics engine with two-way VRML communication for interactive dynamics calculations in near real-time. Also, ITL developed a suite of stand-alone VRML navigation/authoring tools to aid the creation of viewpoints with the addition of sound for multi-modal interaction. The Web site is <http://ovrt.nist.gov/projects/anthrokids/>.

DARPA Intelligent Collaboration and Visualization (IC&V) (20)

In collaboration with the Defense Advanced Research Projects Agency (DARPA), MITRE Corporation,



S. Laskowski and J. Cugini develop prototypes for information visualization in order to measure the effectiveness of various techniques through extensive user testing. (18)

National Imagery and Mapping Agency, and Carnegie Mellon University, ITL is supporting the development of a methodology and software tools to evaluate collaborative systems. The primary task is to define and validate low-cost methods for evaluating collaborative environments, such that researchers in the collaborative computing research community can use these methods to evaluate their own or other research products. We developed a reconfigurable, distributed scripting system that can be used both to develop collaborative tools and to develop test scripts to evaluate collaborative tools. As an example, we used this technology to develop a tool that records and replays events in a Java-based collaborative tool. We also developed a tool for emulating routing packet loss and congestion that could be used for protocol evaluation. The framework developed by ITL is being used as a guide for conducting evaluations for collaborative systems.

Q. Wang and A. Godil discuss the integration issues for a Virtual Reality Modeling Language (VRML) demonstration for manufacturing applications using a dynamics engine and humanoids. (19)

Biometrics - Fingerprint

Three ITL divisions provide technical support to the Information Access and User Interfaces Division to provide the FBI with the research and development efforts required for the creation of standards and specifications relating to the quality, format, and transmission of electronic images and related data over a wide area network. Fingerprint classification and identification allow a reliable means of identifying and storing information about people, whether they are criminals or whether attempting to control their access. NIST's authority as a registered and certified ANSI standards developer allows us to coordinate the development of official ANSI data and image interoperability standards. Such efforts are required in support of the FBI's Integrated Automated Fingerprint Identification System (IAFIS) for the paperless submission, processing, and interchange of electronic fingerprint and mugshot images and data. In FY 1998, we co-sponsored, with the FBI, the Fingerprint Data Interchange Workshop for law enforcement agency staff to re-evaluate the concepts and revise information in the ANSI Fingerprint and Mugshot

Data Interchange Standards. A digital signature will also be considered as part of a revised standard, in anticipation of linking fingerprints to digital signatures. We also released the two-disc Special Database 24, Digital Video of Live-Scan Fingerprint Data. The Web site is <http://www.nist.gov/itl/div894/894.03/fing/>.

Face Recognition

At the request of the National Institute of Justice, ITL is developing standards for evaluating digital video face recognition systems, collecting a standard database of faces in digital video, and implementing and evaluating baseline digital video face recognition algorithms. The transfer of the Face REcognition Technology (FERET) database and FERET evaluation procedures from the Army Research Laboratory to ITL also impacted this project. In FY 1998, we finished and released the September 1996 FERET test report. We developed procedures for collecting a digital video database. ITL also developed a support vector machine-based face recognition algorithm. Industry will benefit by having a standard database available for developing and evaluating face recognition algorithms. A standardized test will also speed commercial acceptance by allowing users to select products with known recognition accuracy. ■

J. Scholtz collaborates with colleagues using Computer Supported Cooperative Work (CSCW) software. Evaluation techniques for CSCW software are being developed by NIST. (20)





J. Roberts subjects a display to stimuli while A. Donohoe and J. Ward review the recorded optical output. (21)

High Performance Systems and Services Division Projects

Advanced Display Technology Systems: Display Image Tolerance Testbed (21)

ITL is developing a measurement methodology that can be used to qualitatively and quantitatively evaluate the performance of a wide variety of information displays. The methodology is applicable to flat panel displays (LCD, plasma, field emission, LED, electroluminescent) for both notebook and desktop monitor configurations, CRT monitors, and projectors (micromirror, LCD, CRT, and light valve). We constructed a prototype device that superimposes a relatively simple noise pattern on the digital signal interface to an active matrix LCD display, thus proving the validity of the method. In FY 1998, we completed the implementation of advanced control and data acquisition using the LabVIEW platform. Manufacturers of flat panel displays (notebook and desktop monitor), systems manufacturers, graphics controller manufacturers, cable and connector manufacturers, and testing laboratories will

benefit from this work. The Web site is http://www.nist.gov/itl/div895/isis/projects/Advanced_Display/.

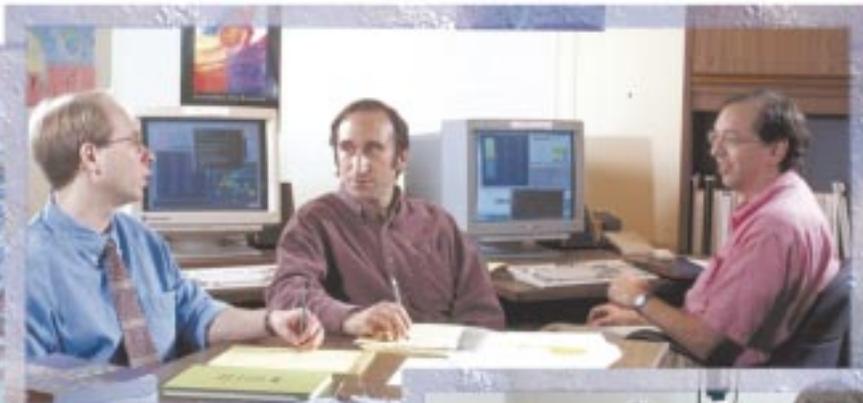
Interoperable Message Passing Interface (IMPI) and Conformance Tester (22)

ITL is facilitating the development of a standard, called IMPI, for interoperability among different MPI implementations. The IMPI standard is being designed by the computer vendors and ITL facilitates the effort, writes the tests, and provides the conformance tester. In FY 1998, we convened three meetings, produced minutes for each meeting, and produced updated draft standards for each meeting. We expect to finish the initial standard by December 1998. The IMPI conformance tester is moving along in parallel. We use a novel approach to the tester by conducting testing over the Web using Java. Vendors connect to the ITL IMPI home page, download the tests, and run the tests between ITL and their MPI implementation. The Web site is <http://impi.nist.gov/IMPI/>.

High Performance Storage Concepts and Standards - Research, Test Methods and Standards for Optical Tape and Optical Disks (23)

In response to the needs of the optical tape industry and other federal agencies, ITL is working with industry to examine technological issues related to the development, implementation, testing, and standardization of emerging data storage technologies such as optical tape and Digital Versatile Disc (DVD). In FY 1998, we enhanced the research and measurement capabilities of ITL's advanced data storage systems laboratory where research is currently conducted on test methods for optical tape media and systems. We implemented DVD and optical tape technology testbeds and interoperability tests. We set up a digital media error test system. We also worked with the U.S. data storage industry to propose a standard metadata specification for portability of sequential storage media systems. The Web site is http://www.nist.gov/itl/div895/isis/projects/Storage_Concepts/.

W. George, J. Hagedorn, and P. Ketcham develop a tool for testing the Interoperable Message Passing Interface (IMPI). (22)



WebSubmit (24)

ITL enhanced WebSubmit, our advanced Internet application tool that provides a Web page interface to supercomputing applications. WebSubmit allows the execution of arbitrary commands and interaction with a user's data files and directories on the target supercomputer as if the user were logged on. The advantage of a Web-based interface is that it is hardware- and software-independent; it depends only on whatever Web browser the user has available. Since WebSubmit was first released in May 1997, we have been working on a second version that is secure, configurable by the system administrator and the user, can submit to multiple computer systems, and works with multiple browsers. In FY 1998, we released the new version of WebSubmit for beta testing at NIST. Currently, it interfaces with the NIST IBM SP2, SGI Origin, and PC Cluster, all of which have different queueing systems. The Web site is <http://websubmit.nist.gov/websubmit.html>.

Computer Time Synchronization (25)

In collaboration with NIST's Physics Laboratory, ITL developed software and hardware techniques to time synchronize computers anywhere in

the world that are connected via a network to within one microsecond accuracy. This is three orders of magnitude better than the one millisecond achieved by current software algorithms over the Internet today. In FY 1998, we completed the construction and testing of a 16-node local time sync device. We also completed the design and construction of the Global Positioning System (GPS) time sync instrumentation and integrated and tested the MultiKron and GPS time sync instrumentation. Finally, we initiated the accuracy testing of the current set of time sync algorithms in local and global environments. Each day, over three million private, academic, and industrial users access and benefit from the NIST one microsecond accurate, time distribution service.

ATM Switch Completion at NIST

As part of the NIST fiber optic backbone service, ITL is upgrading

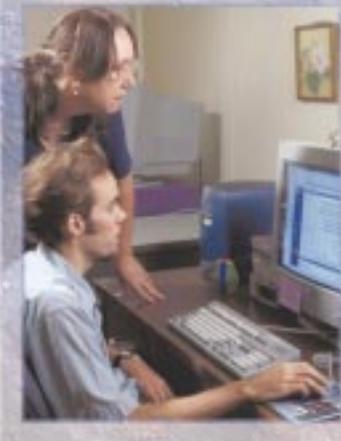


F. Byers and X. Tang test reliability of a digital versatile disc (DVD). Digital information stored on the DVD can be seen on the screen through a microscope. (23)

parts of the network with Asynchronous Transfer Mode (ATM) capability. The ATM backbone currently connects buildings 222, 223, 225, and 820. We are in the process of installing the fiber optic cables from building 223 to building 235 and from building 223 to building 301 for the core ATM connections. NIST backbone subnets will start migrating from FDDI to ATM once the ATM core connections are established among buildings 223, 225, 235, and 301.

Cluster Computing

This ITL project seeks to determine the ability of commodity PC clusters to process the NIST high performance computational workload and to assess the benefits of ATM network



J. Devaney and R. McCormack refine WebSubmit, a secure, configurable, Web-based framework providing seamless access to applications on a collection of networked computing systems at NIST. (24)



B. Hershman adjusts a sensor connection on the NIST GPS time synchronization printed circuit board as directed by A. Mink, R. Carpenter adjusts the oscilloscope tracing the GPS time synchronization pulse and the NIST "trained" time synchronization pulse, and M. Courson plots the time synchronization stability of the NIST GPS "trained" oscillator feeding the NIST MultiKron board which is plugged into a local computer. (25)

technology against Fast Ethernet technology. In FY 1998, we installed, configured, and tested three PC clusters; two clusters were based on 200 MHz Pentium Pro microprocessors and the third was based on 333 MHz Pentium II microprocessors. We used both switched ATM (OC3) networks and switched Fast Ethernet networks to interconnect these clusters, which were instrumented with ITL-developed performance measurement tools. Well-known computational benchmark suites and ITL representative application suites were installed and evaluated. The performance evaluation of this class of clusters showed that they provide a significant level of computation power with a very attractive price/performance ratio.

Optical Information Processing and Transmission: Wavelength-Division Multiplexing (WDM)-Based Photonic Interconnection for Wireless Communications

With the increase in multimedia and the corresponding need for larger bandwidth for wireless communications, an alternative over the use of phase shifting is highly demanded for the receiving and transmission of ground to satellite signals. In collaboration with the Naval Surface Warfare Center, ITL is developing a proof-of-concept experimental WDM interconnection system that can significantly reduce (requiring less than 10 percent of conventional approaches) the

hardware complexity based on our ASTRO 2D TTD architecture. The project also involves the development of a multiple beam and multi-function capability using the architecture. In FY 1998, we characterized the photonic components, implemented an experimental demonstration of WDM, improved the spectral resolution and bandwidth of the acousto-optic tunable DMUX (de-multiplexer) for dense WDM, and achieved an experimental demonstration of an ultrafast image rotation system. The Web site is http://www.nist.gov/itl/div895/isis/projects/Holographic_Storage/. ■



A. Ashcraft and C. Eater test system components while P. Strassberger runs a diagnostics test on a system. (26)

Distributed Computing and Information Services Division

PC Support (26)

At the beginning of FY 1998, the NIST staff switched from outdated office automation software to a modern, integrated suite of software, MS Office. To ease the transition, the PC Support Group conducted many training sessions for NIST staff in the use of the new software. In addition, the group conducted, in Gaithersburg and Boulder, seminars that highlighted the differences between the previous NIST office automation software and the new integrated suite.

A major accomplishment of the PC Support Group was to create a method for NIST staff to automatically install software packages from the Web. PC Support procured a site-wide license for a Windows-based virus detector. This software is available to all NIST staff by simply clicking on an icon on the PC Support Group's Web page. We also developed Web installation packages for Travel Manager, Synchronize, and Eudora.

The group created an entirely new PC Support Web site. More than 75 percent of the current Web site presents new information. Created

from the top down for ease of use, the Web pages offer major categories such as Hardware, Software, Information, Training, What's New, etc. Also available is information on Y2K along with FAQ pages on many of NIST's standard software packages. We also installed a search capability.

To assist NIST staff in dealing with the Y2K problem, PC Support has begun checking the BIOS on all PCs that come in for service. NIST staff may download utilities from PC Support's Web site to perform this test. Staff may also ask PC Support to perform this check.

In the past year, the group improved communications between group members and NIST staff with the goal of improving service across NIST. We implemented an automated customer feedback request covering the quality and timeliness of PC support. All calls are registered in a service tracking database. Once a call is completed, an e-mail message is automatically generated and sent to the customer. The e-mail message contains a link to the survey Web page. After the customer completes the survey and clicks on the "Submit" button, the survey is automatically

received into PC Support's call database. After receiving the survey e-mail, a member of the PC Support group makes a follow-up call to the customer to ascertain that the problem has been corrected and no additional problems have surfaced.

The DOS-based virus detector/remover was replaced with a Windows-based virus detector/remover whose virus list is updated automatically through the Web. This software also detects viruses in e-mail. NIST purchased a site license for the new detector and incorporated the software into a self-installing package accessible through the NIST intranet.

Finally, the group provides installation and maintenance support for NIST's Travel Manager System. Travel Manager grew from a small pilot project to a system that currently services more than 600 users. The use of Travel Manager became mandatory at NIST on April 1, 1998; all NIST staff currently uses Travel Manager to produce authorizations and vouchers. We are testing a new version of Travel Manager that allows NIST to electronically route travel documents.

Administrative Computing Support (27)

In FY 1998, the Administrative Computing Support Group gave top priority to the remediation of NIST administrative systems that were not Year 2000 (Y2K)-compliant. The total Y2K inventory consisted of 113 systems with over one million lines of code, written in COBOL, dBase, FOCUS, and REXX. The majority of these systems support the three primary business units at NIST: the Chief Financial Office, the Office of Human Resource Management, and the Acquisition and Assistance Division. An initial review of the systems showed that 42 percent of the systems were Y2K-compliant and required no modification. By the end of the fiscal year, 53 percent of the systems had been renovated, raising the level of compliance to 95 percent. The group gave special attention to external data exchanges and the Y2K compliance of the external system and the data being exchanged. In addition, we analyzed the compliance of the mainframe IBM and Unisys hardware platforms and upgraded their operating systems, compilers, and associated utility programs to Y2K-compliant levels.

The group supported the Department of Commerce Administrative Management Systems (CAMS) project. The CAMS effort may be viewed as the Core Financial System (General Ledger, Accounts Payable, etc.) and supplementary modules to be developed by NIST and other DoC

agencies. In FY 1997, NIST agreed to lead the development of two supplemental modules, a Personal Property module and a Time and Attendance/Estimated Labor module. Both modules were completed in FY 1998. The Personal Property Module was implemented in May 1998 using the COTS Oracle Fixed Assets. The new system replaced a 15-year-old legacy system.

As a step in preparing for CAMS as well as strengthening the current financial system, the Vendor Table from CAMS was implemented to serve as the Vendor Table for NIST's current system. This allows NIST to prepare to meet the Debt Collection Improvement Act, which mandates Electronic Funds Transfer to vendors as well as 1099 reporting for the IRS.

In addition to the Y2K project and the two CAMS Modules projects, the group continued to support the business operations of the 100+ administrative computing systems at NIST. This included revising DOS-based systems to be Windows 95-compatible, responding to auditors' requests, and developing Web pages for system users.

Distributed Processing and Operating Systems Support

For FY 1998, the Distributed Processing and Operating Systems Support Group maintained the high level of availability of the services provided to NIST staff in the past. In addition, we created a new project



D. Osborne tests software for verifying the ability of PCs to properly process dates after 1999. (27)

team to provide Windows NT support. A Windows NT NIST-wide Enterprise Architecture was developed that uses a Master NIST Domain Controller and permits the inclusion and support of current domains in Gaithersburg and Boulder laboratories. The new architecture provides improved security and permits data interchange between NT and UNIX servers. The members of the team provide consulting assistance to NIST scientists and engineers and administer NT servers for other NIST operating units on a fee basis.

The electronic mail servers operated by the group for NIST staff in Gaithersburg and Boulder continued to provide highly reliable service to over 2,900 users. Over 30,000 e-mail messages are processed each day. These same servers managed the translation of over 5,000 generic NIST e-mail aliases, most in the form of `firstname.lastname@nist.gov`, to the actual addresses to which mail is delivered. These servers also were used to administer and process messages to over 250 mailing lists used by NIST staff to distribute messages to subscriber lists. These

lists range in size from ten users to the entire NIST staff at Gaithersburg and Boulder.

The group continued to operate three other servers supporting applications accessed by NIST staff:

- the Usenet News server, giving staff access to over 25,000 special-interest Internet discussion groups;
- a software checkout server providing NIST staff with access to expensive, licensed data processing software packages; and
- a Sun Microsystems Enterprise 4000 computer system acting as a file server to computers running both the UNIX and Microsoft Windows operating systems.

Information Processing Support

In FY 1998, the Information Processing Support Group began a number of new initiatives while continuing to provide support of NIST's centralized World Wide Web (Web) servers. One initiative implemented a pilot Public Key Infrastructure (PKI) for ITL. A PKI

pilot system was developed using a commercial Lightweight Directory Access Protocol (LDAP) server and certificate generation software. The system will be tested initially by ITL managers and secretaries and allow them to digitally sign, encrypt, or sign and encrypt e-mail. The system will also be used on the Web to authenticate WebSubmit users.

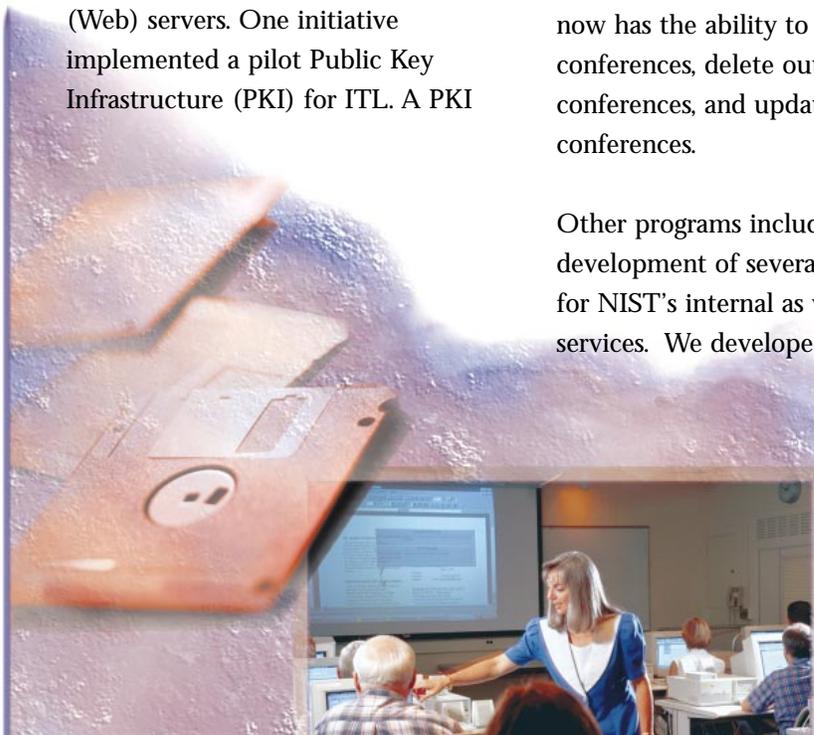
The electronic commerce system developed and placed in operation in FY 1997 was expanded to provide an online conference registration page. This gave NIST's Conference Facilities the ability to accept conference registration and payment via the Web. As COTS software to meet NIST requirements was not available, the group developed the software, configured the system, and implemented the security procedures to ensure that the information taken was handled securely and was properly routed to the correct NIST contacts. Conference Facilities now has the ability to add new conferences, delete outdated conferences, and update existing conferences.

Other programs included the development of several Web sites for NIST's internal as well as external services. We developed Web sites that

have specific functionality. One example is the implementation of a site for NIST's Operations Board, which consists of Laboratory Deputy Directors. The site includes an online calendaring system, file upload capability, and discussion groups and can be accessed by members of the board only. The Operations Board uses the site to quickly disseminate information and to discuss pertinent issues. Another example is the "Successful Practices for DoC Acquisition." This site allows DoC acquisition employees to enter information about general successful practices. Other functionality includes allowing other agencies to browse, search, and provide feedback on information stored in the site database. The site also alerts subscribers when new information is entered. Along with the public access site, an internal, limited access site permits specific acquisition officers to maintain and reconfigure the site.

The group provided NIST with Web consulting on technical questions as well as Web page design questions. Questions were primarily sent via e-mail to Webmaster@nist.gov. Consultations were provided on Web-to-database applications, including a chemical waste reporting form and a Solicitation Mail List Application. These database applications support both Internet and intranet users. Applications are stored on centrally maintained systems that are continuously monitored by software. ■

L. Helfer presents customized classes for NIST staff transitioning to new in-house standard software. (26)



Software Diagnostics and Conformance Testing Division Projects



M. Kass and M. Brady discuss design issues for the VRML Test Suite (VTS), a unique Web-based metrology tool used by industry partners to determine conformance to the Virtual Reality Modeling Language (VRML). (28)

Virtual Reality Modeling Language (VRML) Conformance Testing (28)

VRML is the file format standard for 3D-multimedia and shared virtual worlds on the Internet. We developed the VRML Test Suite (VTS) system and Viper, a VRML reference parser and scene graph generator. Work continues in populating the VTS with additional test cases and in building a dynamic testing capability. In FY 1998, we continued the development of VTS semantic requirements, test cases, and expected results. We enhanced Viper to flag minimum conformance file limits and to handle Scripts. Finally, we defined an approach for VRML dynamic testing and developed a pilot automated testing capability. The Web site is <http://www.nist.gov/vrml.html>.

Technology Transfer of Conformance Testing Programs (29)

ITL refocused its program on the development of conformance tests for new, emerging information technologies rather than on operational testing services. We are working with industry to transfer knowledge of testing, provide help in the use of ITL-developed test suites, and assist industry in establishing testing programs and services. By the end of FY 1998, all

ITL-operated software validation testing services were terminated. We also developed conformance testing methodologies that are being transferred to industry. The Web site is <http://www.nist.gov/ctdirectory.html>.

Role Based Access Control (RBAC) (30)

Working with our Computer Security Division, Software Diagnostics and Conformance Testing Division researchers developed an implementation of RBAC for Web servers, called RBAC/Web. In FY 1998, we completed the RBAC/Web server software and made it available online. We are testing tools for managing user roles and role-privilege links and expect to complete and release these tools early next year. Participants include George Mason University, the University of Maryland, and the National Security Agency. In addition, under a CRADA, SETA Corporation is porting and extending NIST's existing RBAC administrative tool for use in SQL environments as a part of their commercial software. The Web site is <http://hissa.ncsl.nist.gov/rbac/>.

Object Oriented Technology for Distributed Interactive Learning (31)

This project focuses on the development, evaluation, and demonstration of distributed object

technology and Learning Object (LO) metadata as key enablers for developing interactive, distributed learning systems. In collaboration with EDUCAUSE's Instructional Management System (IMS) project, ITL participates in defining a framework of services and interfaces for learning systems, including RBAC services, and will implement and test selected services within an ITL testbed as part of a distributed object-based IMS system prototype. We developed the original metadata specification and in FY 1998, we demonstrated the prototype Web-based metadata and repository capabilities. The metadata repository

J. Schneider, P. Himes, and S. Sherrick examine test results in order to provide feedback to a vendor who has executed the NIST CGM conformance test suite. (29)

NIST developed an RBAC model, specified using formal methods and implemented for the Web, that includes role hierarchies and separation-of-duties features. J. Barkley shows the tools to S. Gavrila, W. Majurski, T. Cincotta, and R. Kuhn. (30)

will be integrated with other tools and tested within the IMS prototype system. These evaluations will demonstrate and validate key technologies and specifications and promote adoption by industry and standards organizations.

Automatic Generation of Tests From Formal Specifications (32)

A competency effort to improve the state of the art in automated test generation, this project focuses on the development of methods to produce software tests, including conformance tests, from formal specifications. These methods promise significantly more economical means for testing software than are currently available. This reduces time-to-market for companies producing software products. In FY

1998, we created a formal specification of an automobile cruise control, inserted faults in the specifications, used a model checker to check the faulty specifications, and generated counter examples (test cases) which detected the fault. We ran test cases on an implementation written in Java and examined the resulting coverage to determine if some tests led to better coverage. The Web site is <http://hissa.nist.gov/~black/FTG/autotest.html>.

Java Testing (33)

In response to industry's need for conformity assessment methods to ensure consistency and accurate use of the Java specification, ITL initiated a Java testing project. In September 1997, we hosted the Java Conformance Assessment Workshop which identified four areas of research and market need where ITL could make a contribution: NIST Test Cases for Java; Real-time

Issues in Java; VM View; and JavaCard Verification. In FY 1998, we released Version 1.0 of VM View, providing trace capability for post-processing analysis. We hosted the Workshop for Real-time Issues in Java Implementations in June 1998. This workshop resulted in an ITL-led working group, which is producing a set of requirements for real-time Java. ITL also explored with smart card vendors and the JavaCard Forum, development of a formal description and generation of tests of the Java Card Virtual Machine specification. Industry partners include Sun Microsystems, Hewlett Packard, IBM, Plum Hall Inc., IEEE Computer Society, the Defense Information Systems Agency's Center for Standards, and Gemplus. The Web site is http://www.nist.gov/java_ca.htm.

Software Testing by Statistical Methods (34)

In this competency project, ITL is developing new methods for software testing based on stochastic processes and statistical measures in order to improve the quality of software and to provide quantitative measures for determining the probability that software correctly adheres to its specifications. In FY 1998, we investigated the applicability of statistical techniques

Y. Yesha (UMBC), P. Ammann (GMU), and P. Black discuss automatic generation of software tests from formal specifications. (32)



E. Fong and T. Rhodes develop metadata and a Web-based metadata registry for instructional content. (31)



L. Carnahan and A. Dima compare designs of new features for VM View, a diagnostic trace tool developed at NIST for Java programs. (33)

Statisticians and computer scientists, C. Hagwood, L. Gallagher, L. Rosenthal, J. Yen, D. Banks, and R. Kacker, seek new quantitative methods for determining the probability that software correctly adheres to its specification. (34)

to software testing. We identified subtopics for in-depth investigation and prototyping including reliability of conformance tests, clinical trials, and bug simulation. We initiated, designed, and developed protocol simulation and comparison. Also investigated was the application of a domain-based input sampling strategy to the CGM conformance test suite. The Web site is <http://www.nist.gov/stsm.html>.

Error, Fault, and Failure Data Collection and Analysis

Responding to the needs of industry and the research community, ITL is acquiring error, fault, and failure data to develop profiles for industry use and for statistical analysis methods. The collection and analysis of software data may yield reference data for matching development and assurance methods to characteristics of a specific system. In FY 1998, we developed an initial, Web-based data collection and analysis tool, the EFFTTool, which is a collection tool for operational failures. We anticipate the public release of the database in 1999. Project participants include SoHaR, Inc., under a CRADA and RST Corporation under the Advanced Technology Project. The Web site is <http://hissa.nist.gov/project/eff.html>.

Requirements Collection for Forward-Looking Standards

ITL is collecting, coordinating, and disseminating federal government technical requirements for cutting-edge software technology. Working with other federal agencies, we ensure that these requirements are made known to the appropriate voluntary standards community organizations. In FY1998, we participated in the development of the charter for a new "standards" organization under the Federal Government's Chief Information Officer (CIO) Council Interoperability Committee. ITL provides the chairperson and necessary support personnel for the Standards Working Group under the CIO Interoperability Committee.

Unravel

ITL built a tool called Unravel that reduces the time and effort needed to analyze programs for maintenance or testing, measured in terms of lines of code. Consisting of an analyzer, a linker, and a slicer, the tool was developed in C. In FY 1998, ITL made available online a complete version of Unravel. Software developer BAI, Inc., adapted

Unravel to create a commercial product designed to speed up software changes required to deal with year 2000 problems. We are developing a Java version for release in 1999. The Web site is <http://hissa.ncsl.nist.gov/~jimmy/unravel.html>.

Year 2000 (Y2K) Software Problem Information Dissemination

To assist government and industry in dealing with Y2K issues, ITL provides a source of unbiased information concerning techniques that can be used to resolve Y2K software problems. In June 1997, we co-sponsored the "International Symposium on the Year 2000 - Mastering the Millennium Rollover." We also assisted in the development and implementation of training materials for NIST's Manufacturing Extension Partnership Conversion 2000: Y2K Program. We developed several Web-based software programs that can be used by organizations to evaluate their legacy software to determine the amount of potential exposure to Y2K failure. By the end of FY 1998, our Y2K Web site provided information and software to over 22,000 visitors. The address is <http://www.nist.gov/y2k>. ■



L. Gill consults with J. Brown Thomas (CSTL) on the analysis of a Standard Reference Material. (35)

Statistical Engineering Division Projects

Statistical Reference Datasets (StRD)(35)

ITL developed a Web-based service that provides reference datasets, together with certified values for the results of statistical computations, for a variety of statistical methods. Industries benefiting from the reference datasets include those that use statistical software, especially the information technology, pharmaceutical, chemical, electronic, automotive, and aerospace industries.

The service currently provides 58 datasets with certified values for assessing the accuracy of software for univariate statistics, analysis of variance, linear regression, and nonlinear regression. The collection includes both generated and "real-world" data of varying levels of difficulty. Generated datasets are

designed to challenge specific computations. The service is available at <http://www.itl.nist.gov/div898/strd>.

We released the StRD Web service to the public in August 1997. The Web site is being used extensively, averaging 1500 hits per month in 1998. Some vendors are retooling their packages to improve performance based on the datasets. In FY 1998, we began compiling a NIST Technical Report documenting the development of the StRD Web service, to be published in 1999. Feedback from users will be considered to enhance and improve StRD Web services in the future.

Rockwell Hardness Standards (36)

In today's metal products and materials industries, hardness testing is the most

widely used mechanical test for quality control and acceptance testing. Even so, worldwide unification and standardization of any hardness scale are yet to be accomplished. Furthermore, prior to the start of this NIST project, no Standard Hardness Reference Scale within the U.S. was traceable to national standards. The primary goals of the project are to provide U.S. industry with a means to make hardness measurements and calibrations with traceability to national standards, and to facilitate acceptability of American hardness measurements worldwide. From a statistical perspective, NIST's objective is to enable people who do hardness measurement to judge the uncertainty in their measurements. This involves making available SRMs for the Rockwell C Scale, providing tutorials on experiments for judging the errors in hardness measuring

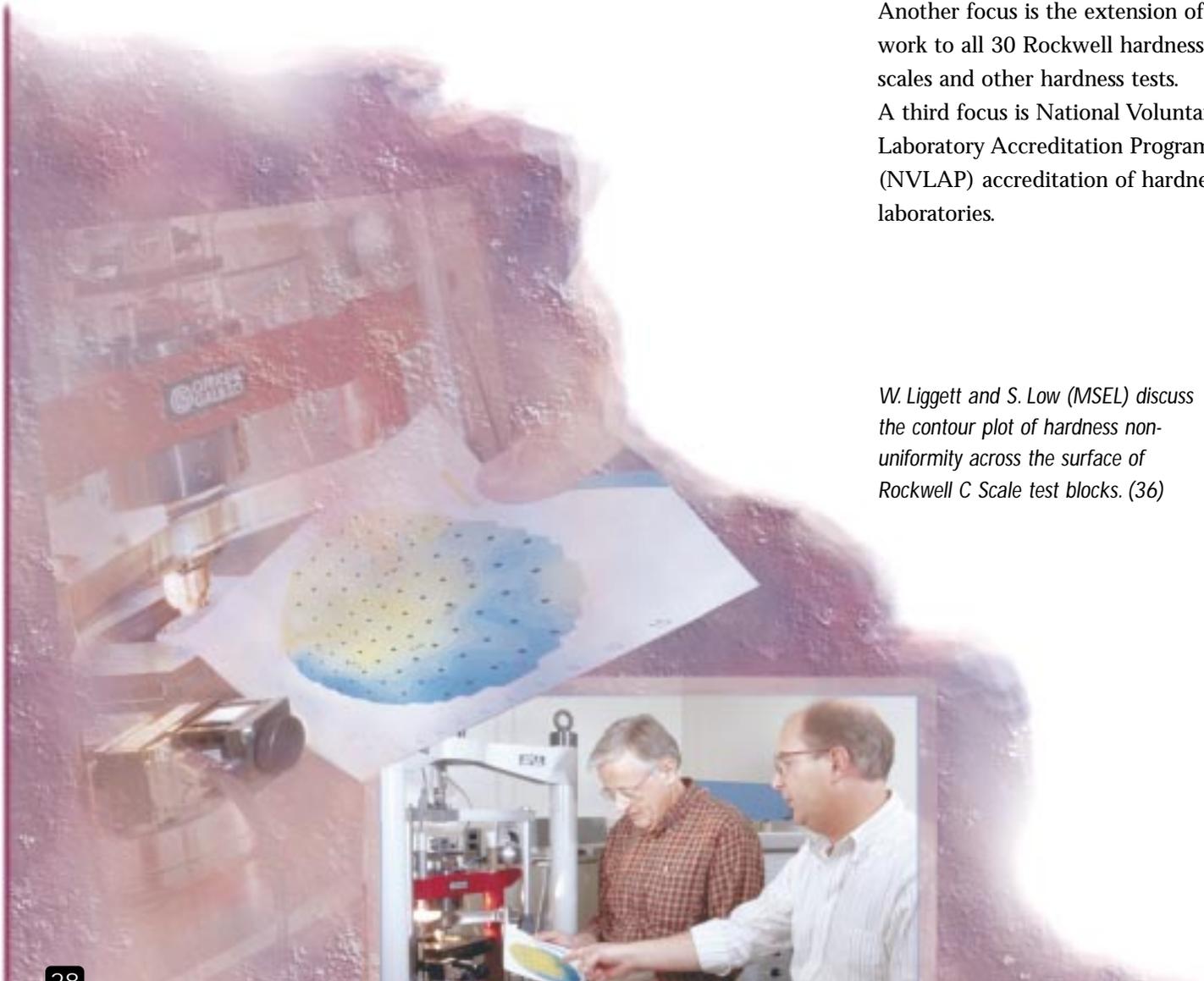
systems, and extending this effort to other Rockwell scales.

In collaboration with the Materials Science and Engineering Laboratory and the Manufacturing Engineering Laboratory, ITL contributed a fundamental change in the way hardness test blocks are used and consequently, a major change in the way measurements on test blocks are interpreted. NIST SRMs for the Rockwell C Scale went on sale in June 1998. With the issuance of the NIST

SRMs, what is considered a correct hardness measurement has shifted by about one half Rockwell point. This change has been accepted by the hardness testing community because it brings U.S. measurements into line with Japanese and European measurements. Rockwell C Scale hardness measurement is primarily used in judging the heat treatment of steel. For the manufacturers involved, NIST's work has provided traceability and comparability with measurements made in the U.S. and in other countries.

A workshop on hardness standardization held in June 1998 drew 200 people who do hardness testing. A publication on hardness measurement experiments is in draft form and will be available for the tutorial to be presented at the Measurement Science Conference in January 1999. We are currently working to achieve acceptance of new ways of assessing the error in hardness testing systems. Work on SRMs for the Rockwell B Scale is beginning. Future work will focus on achieving consensus in the proper ASTM committee on the steps in upgrading hardness measurement. Another focus is the extension of the work to all 30 Rockwell hardness scales and other hardness tests. A third focus is National Voluntary Laboratory Accreditation Program (NVLAP) accreditation of hardness laboratories.

W. Liggett and S. Low (MSEL) discuss the contour plot of hardness non-uniformity across the surface of Rockwell C Scale test blocks. (36)



NIST/SEMATECH Engineering Statistics Internet Handbook (37)

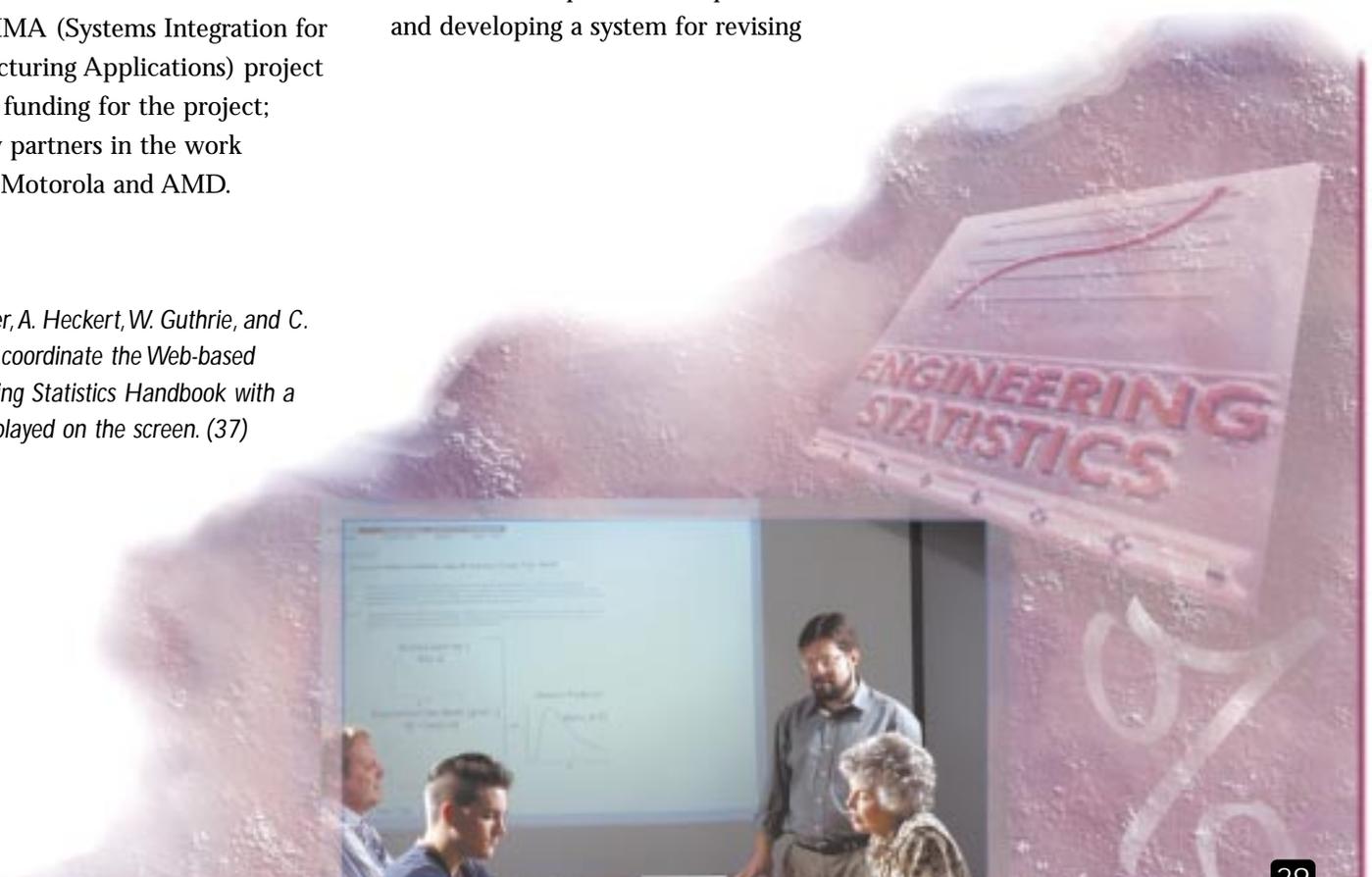
Under a cooperative research and development agreement (CRADA) established in 1995, ITL and SEMATECH are collaborating in the development of an online Handbook of Engineering Statistics for distribution on the Web. The handbook will be readily available and useful to engineers and scientists in industry and will enable them to incorporate statistical methods into their work more efficiently. By extending the benefits of modern statistical design and analysis to the engineering and scientific communities, the online resource will contribute to the productivity and competitiveness of U.S. industry in the global marketplace. SEMATECH and the NIST SIMA (Systems Integration for Manufacturing Applications) project provide funding for the project; industry partners in the work include Motorola and AMD.

M. Reeder, A. Heckert, W. Guthrie, and C. Croarkin coordinate the Web-based Engineering Statistics Handbook with a page displayed on the screen. (37)

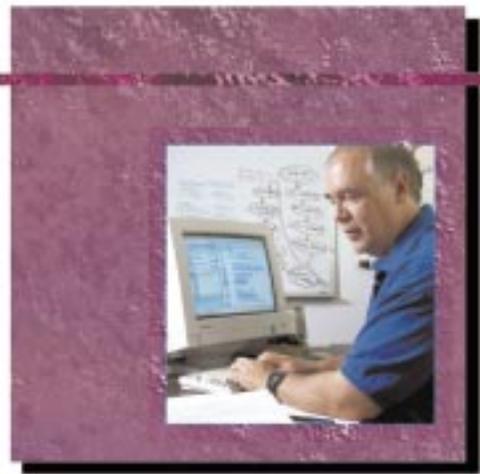
Using a problem-oriented approach, the handbook will describe detailed case studies from the semiconductor industry and the NIST laboratories that illustrate statistical approaches to solving engineering and scientific problems. The treatment of examples has evolved from reliance on detailed calculations with explicit formulas to graphical and analytical results from statistical software packages. Handbook users will be able to use commercially available statistical software to run an analysis on their own data similar to the analysis in a case study and then compare the results and interpretations.

With the design of the handbook completed in 1997, we focused in FY 1998 on creating chapter pages, putting together case studies with interactive computational capabilities, and developing a system for revising

and updating the document. We also solicited feedback from usability studies conducted at the 1998 International Conference on Characterization and Metrology for Ultra Large Scale Integration (ULSI) Technology, held at NIST, and at the spring SEMATECH Statistical Methods Group Symposium. Early in FY 1999, the handbook will be released for beta testing at NIST and SEMATECH, with public release scheduled later in the year. For more information, visit the Web site at <http://www.itl.nist.gov/div898/projects/handbook.html>. ■



Industry Interactions



J. Lyle uses Unravel, a program slicing tool developed at NIST, to extract all the statements relevant to a single computation.

ITL establishes partnerships with industry, academia, and government to pursue research areas of mutual interest. Through Cooperative Research and Development Agreements (CRADAs), we worked with 48 organizations in FY 1998. For information on our participation in voluntary standards activities, see <http://www.itl.nist.gov>. ITL also participated 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, 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. Lynne Rosenthal is the ITL contact.

American National Standards Institute (ANSI)

ANSI serves as administrator and coordinator of the United States private sector voluntary standardization system. Michael Hogan and Christopher Dabrowski participate in the Information Infrastructure Standards Panel (IISP) and Carroll Croarkin serves on the ASC Statistics Subcommittee. Hogan also participates on the ANSI Information Technology Consultative Committee (ITCC).

Association for Computing Machinery (ACM)

ACM is the world's oldest and largest educational and scientific computing society. Since 1947, ACM has provided a vital forum for the exchange of information, ideas, and discoveries. Ronald Boisvert serves on the ACM Publications Board and John Barkley participates in the Role Based Access Control working group.

Association for Information and Image Management (AIIM) International

ITL participates in AIIM, the world's leading global association for information management professionals and providers of digital document technologies. AIIM is an accredited American National Standards Institute (ANSI) standards development organization involved in creating, disseminating, and promoting industry standards worldwide. Fernando Podio represents ITL on AIIM's Committee C21, Storage Devices and Applications.

ASTM

ASTM (American Society for Testing and Materials) is a not-for-profit organization that provides a forum for producers, users, ultimate consumers, and those having a general interest (representatives of government and

academia) to meet on common ground and write standards for materials, products, systems, and services. Carroll Croarkin participates in Technical Committee E-11, Quality and Statistics.

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 telecommunications corporations comprise the forum. Through the forum, ITL works with test equipment vendors and ATM switch vendors to develop interoperability test specifications and conformance test suites. David Su, Leslie Collica, and David Cypher represent ITL in the ATM Forum.

Basic Linear Algebra Subprograms (BLAS) Technical Forum

The BLAS Technical Forum is an industry/government/academic working group, which is developing community standards for sparse matrix kernel and extending the BLAS to new domains. This work includes the development of interface specifications, reference implementations, and a project Web site. Roldan Pozo and Karin Remington represent ITL. Pozo chairs the sparse matrix subcommittee.

Center for National Software Studies (CNSS)

The CNSS is an organization of software professionals who recognize the need for national focus and informed leadership on software issues. ITL works with the CNSS to identify issues that affect the software capability of the nation; CNSS's initiatives include national competitiveness, trustworthiness of software systems, and competency of the software workforce. Shukri Wakid and Dolores Wallace represent ITL.

CommerceNet Consortium

CommerceNet is an industry association for Internet commerce whose mission is to make electronic commerce easy, trusted, and ubiquitous. ITL is one of 500 members of the organization, which approaches all issues from a multidisciplinary perspective encompassing technology, business processes, and regulatory policies. Bruce Rosen is the ITL contact.

Common Criteria (CC) Implementation Board (CCIB)

The CC represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. Eugene Troy and Stuart Katzke represent ITL in the implementation process.

Cross Industry Working Team (XIWT)

The 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

D. Cypher, L. Collica, and Y. Song configure and connect Asynchronous Transfer Mode (ATM) switches in order to test Private Network-Network Interface (PNNI) interoperability using an analyzer and automated test sequences.



computer, networking, telecommunications, publishing and banking sectors, and others with business interests in the NII. Shukri Wakid and R.J. (Jerry) Linn represent NIST on the executive committee; other ITL representatives participate in working groups related to their research and development activities.

Digital Audio Visual Council (DAVIC)

DAVIC is an international consortium for 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. The ITL principal is Karen Hsing.

ECMA

ECMA is an international, Europe-based industry association founded in 1961 and dedicated to the standardization of information and communication systems. Gary Fisher participates in the Java Scripting Language Study Group.

EDUCAUSE

EDUCAUSE is a consortium of university and industry providers of educational material. ITL's work with EDUCAUSE resulted in the adoption of NIST's Role Based Access Control model for the EDUCAUSE Instructional Management System (IMS) application program interface. Shukri Wakid, John Barkley, and

M. Zimmerman and D. Wallace collect data from problematic computer-based systems and develop profiles characterizing software systems. Problems traced to software faults are analyzed according to observed behavior, cause of the software problem, type of device, and other factors.

Tom Rhodes serve as advisors to the EDUCAUSE IMS consortium.

Forum of Incident Response and Security Teams (FIRST)

FIRST is an international coalition of government, industry, and academia whose purpose is to share information on information security vulnerabilities and attacks. John Wack represents ITL.

G8 Information Society

G8 is a coalition of eight major industrialized nations. Its mission is to build on and sustain the process of globalization and to ensure that its benefits are spread more widely to improve the quality of life of people everywhere. ITL provided leadership in planning, developing, and implementing the U.S. contributions to two of the eleven Information Society Pilot Projects: the Global Inventory Project (GIP) and the Global Marketplace for Small and Medium Enterprises (SMEs). Judi Moline serves as the U.S. representative to the two steering committees.

Information Infrastructure Standards Panel (IISP)

Sponsored by the American National Standards Institute (ANSI), the IISP is an open forum, which accelerates the development of standards critical to the deployment of information infrastructure products and services. Participants include a broad spectrum of companies,



government agencies, standards and specifications-developing organizations, industry associations, and consortia. ITL has actively contributed to the fulfillment of IISP's mission since its inception. Michael Hogan represents ITL.

Information Infrastructure Standards Panel (IISP) Steering Committee

The IISP Steering Committee consists of representatives from six industry consortia, twelve corporations, and three government agencies. The Steering Committee ensures that the business of the IISP is accomplished effectively and the decisions of the IISP are carried out. ITL's Michael Hogan represents the National Committee for Information Technology Standardization (NCITS) on the IISP Steering Committee; Shukri Wakid represents NIST.

Information Technology Industry (ITI) Council

ITI is an industry association that represents the leading U.S. providers of information technology products and services. It promotes the global competitiveness of its 30 member companies. ITI serves as the secretariat for the American National Standards Institute (ANSI) Accredited National Committee for Information Technology Standards (NCITS) and as U.S. Technical

Advisory Group (TAG) administrator for ISO/IEC Joint Technical Committee 1 on Information Technology. The ITL liaison is Michael Hogan.

Institute of Electrical and Electronics Engineers (IEEE)

IEEE is the world's largest technical professional society. IEEE focuses on advancing the theory and practice of electrical, electronics and computer engineering, and computer science. David Su participates in P802.14 Cable Modems. Shukri Wakid serves on the IEEE Computer Society Technical Advisory and Publications Boards. Daniel R. Benigni was Vice President for Regional Activities for 1998 and is the ITL liaison to the IEEE Standards Association Board of Directors.

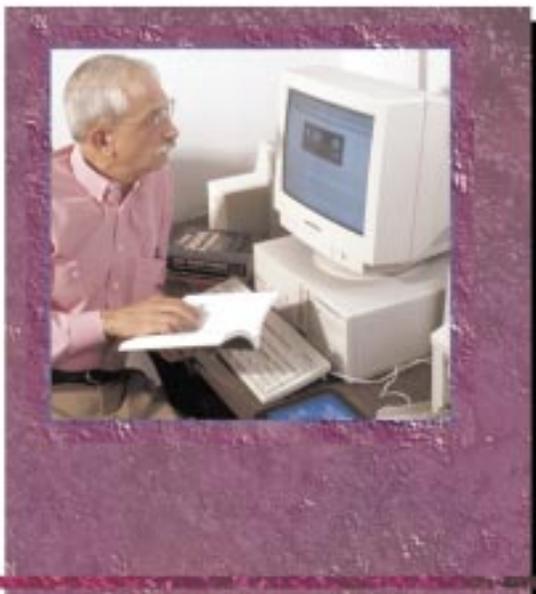
Interactive Multimedia Association (IMA)

IMA promotes the development and use of interactive multimedia worldwide. Thomas Rhodes represents ITL on the working group for the metadata standard for digital objects.

International Federation for Information Processing (IFIP)

ITL participates in the IFIP Working Group on Numerical Software (WG 2.5), which is part of the IFIP Technical Committee on Programming Languages (TC 2). The Numerics Working Group is chartered to be the voice of the community on changes to Java which would make it suitable for numeric-intensive applications, as well as a center of coordination for the development

G. Fisher coordinates NIST standards and testing activities concerning the year 2000 computer problem. A major emphasis is creating awareness of the issues and possible solutions for overcoming the problems associated with converting systems and testing them for compliance with year 2000 date processing requirements.



of community-supported class libraries and interfaces for core numerical computations. Ronald Boisvert represents ITL.

International Information Integrity Institute (I4)

This international organization consists of the senior IT security managers from large, global organizations. NIST is a U.S. Government representative in I4. I4 is managed by SRI Consulting, which conducts meetings (three per year), produces regular technical reports, and undertakes special research projects. The I4 forum provides a means for discussion of a wide range of computer security issues with large IT providers and users. Stuart Katzke represents ITL.

Internet Engineering Task Force (IETF)

The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. ITL actively participates in the Internet Area (IPv6, IP/ATM), the Management Area (SNMP, MIBs), the Routing Area, the Security Protocols Area, the Transport Area (RSVP, RTP), and the Privacy and Security Research Group. Doug Montgomery is the ITL contact for general issues related to the IETF and for reference to further points of contact on specific issues.

Internet Society (ISOC)

The Internet Society provides leadership in addressing issues that confront the future of the Internet. It is the organizational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). Doug Montgomery and Craig Hunt represent ITL.

Java Grande Forum

The Java Grande Forum (JGF) is an open forum of industrial, government, and academic researchers, and software developers interested in improving the Java language and environment for use in high performance computing. Roldan Pozo and Ronald Boisvert co-chair the Numerics Working Group.

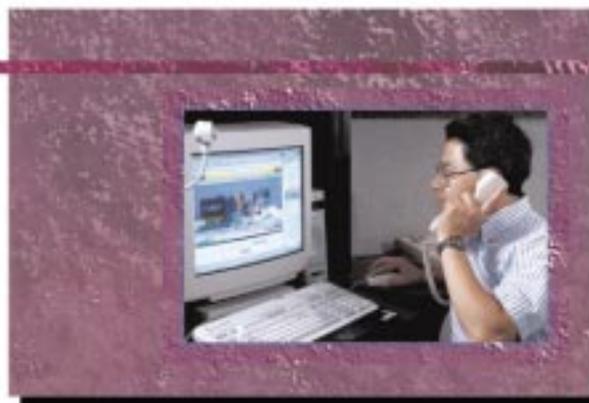
Micromagnetic Modeling Activity Group (muMAG)

MuMAG is an organization of industrial, government, and academic researchers investigating fundamental issues in micromagnetic modeling through two activities: the establishment of standard problems for testing micromagnetic simulation software and the development of a public domain reference implementation of micromagnetic simulation software. In August 1998, ITL co-sponsored a regional workshop of muMAG in Boulder, Colorado. James Blue, Michael Donahue, and Donald Porter represent ITL.



J. Newton and B. Rosen develop a Web-based online system to support the collection of federal government requirements for technical software standards.

W. Chang uses Streaming Synchronization MultiMedia (S2M2) SMIL player to discuss the SMIL interoperability testcase scenarios with other SMIL scientists from Lucent Technologies, RealNetwork, Compaq, and Philips. S2M2 is a NIST reference implementation of the SMIL Recommendation from World Wide Web Consortium (W3C). S2M2 allows Java-enabled browsers to present temporal and spatial synchronization of Web multimedia objects such as audio, videos, images, and text to create richer TV-like multimedia content.



MultiMedia Communications Forum (MMCF)

The MMCF is an international industry consortium dedicated to the goal of accelerating market acceptance of multimedia communications equipment from multiple vendors, with this equipment interoperating across different types of networks. The MMCF is committed to a broad systems approach through the creation of specifications, the education of the industry, and through alliances with other industry groups working toward complementary objectives. Shukri Wakid serves on the MMCF Board.

North American Integrated Services Digital Network (ISDN) Users' Forum (NIUF)

The NIUF is an industry/government consortium designed to create a strong user voice in the implementation of ISDN applications. Through the NIUF, users and manufacturers concur on ISDN applications and the resolution of issues, enhancing the strength of the U.S. telecommunications industry in the world marketplace. ITL's Leslie Collica chairs the NIUF and Sara Caswell serves as NIUF Secretariat.

North American Interoperability Policy Council (NAIPC)

NAIPC provides the North American focal point for the development, coordination, and harmonization of

policy as it pertains to demonstrating interoperability for information technology and telecommunications products worldwide. Michael Hogan represents ITL on this council.

North America OpenMath Initiative (NAOMI)

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

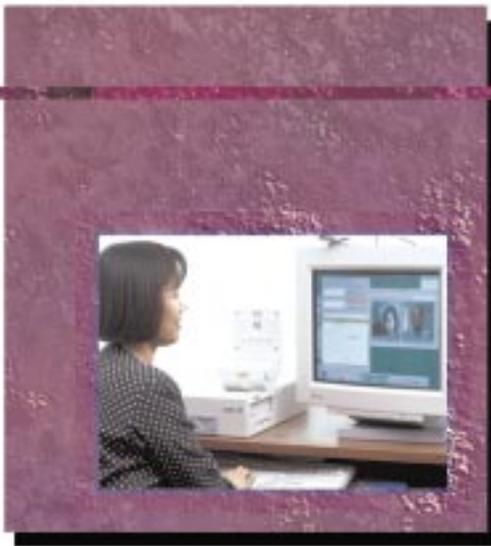
Object Management Group (OMG)

The OMG is a nonprofit international consortium of 500 organizations whose mission is to research, develop, and promote the use of object-oriented technology for distributed systems development. The membership consists of all the major producers of information technology hardware and software, large user organizations, government agencies, and universities. ITL contributes to seven working groups within OMG. A member of the OMG Object Management Group, John Barkley is ITL's principal representative.

OPEN GROUP

The OPEN GROUP was established to aid in the development and implementation of a secure and reliable IT infrastructure. Shu-Jen Chang participates in Security Services. The group focuses on the provision of security at three levels: a secure Internet, a secure corporate network, and secure computing platforms, with key focus

O. Kim tests the Java Collaborative Environment (JCE) framework that provides an integrated platform-independent multimedia desktop conferencing system.



areas that include Public Key Infrastructure and Single Sign-On, a means of using one log-on for all enterprise network systems.

Software Engineering Body of Knowledge Industrial Advisory Board

ITL serves on the Industrial Advisory Board for the ACM and IEEE Computer Society's project to develop a Software Engineering Body of Knowledge (SWEBOK). The purpose of the SWEBOK is to identify the body of knowledge of software engineering and to provide suitable access to that knowledge. The expected customers are licensing and certification agencies, accreditation boards, software professionals, and others who wish to understand the responsibilities of software engineers. Shukri Wakid, Dolores Wallace, and Larry Reeker represent ITL.

Software Engineering Institute (SEI)

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 with SEI to work collaboratively on software engineering issues of mutual interest. Under this agreement, SEI supports ITL in its Software Error, Fault and Failure Data Repository project in acquiring and in developing software collection and analysis tools. Dolores Wallace is the ITL principal.

Video Electronics Standards Association (VESA)

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

Virtual Reality Modeling Language (VRML) Consortium

The VRML Consortium was formed to provide a forum for the creation of open standards for VRML specifications, and to accelerate the worldwide demand for products based on these standards through the sponsorship of market and user education programs. Through participation in the VRML Consortium, ITL works with industry to develop conformance tests and test tools for VRML. Lynne Rosenthal represents ITL.

World Wide Web Consortium (W3C)

The W3C is an international industry consortium created to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. Wo Chang and Tim Boland represent ITL. ■

International Activities

Assistance to Singapore on Information Technology Security Issues

ITL continued its long-standing collaboration with government and private organizations in Singapore. In October 1997, Stuart Katzke, Chief, Computer Security Division, met with six different groups including standards working groups, government departments, the Productivity and Standards Board which provides testing and metrology services to the Singapore government, and the banking industry. Discussions centered on current security issues including cryptography, the establishment of a Common Criteria Testing Program, the National Information Assurance Partnership (NIAP), the establishment of a security evaluation program and scheme in Singapore similar to those in other countries, and the security of financial systems.

ATM Network Technology Collaboration with Korea

Through a Memorandum of Understanding, ITL, the Korea Telecom Research Group (KTRG), and the Electronics and Telecommunications Research Institute (ETRI) are jointly developing abstract conformance test and interoperability test suites for ATM network protocols and Video-on-Demand (VoD) service. KTRG and ETRI assigned guest scientists to work at NIST with ITL researchers in developing test suites and VoD reference implementations. In FY 1998, Karen Hsing of

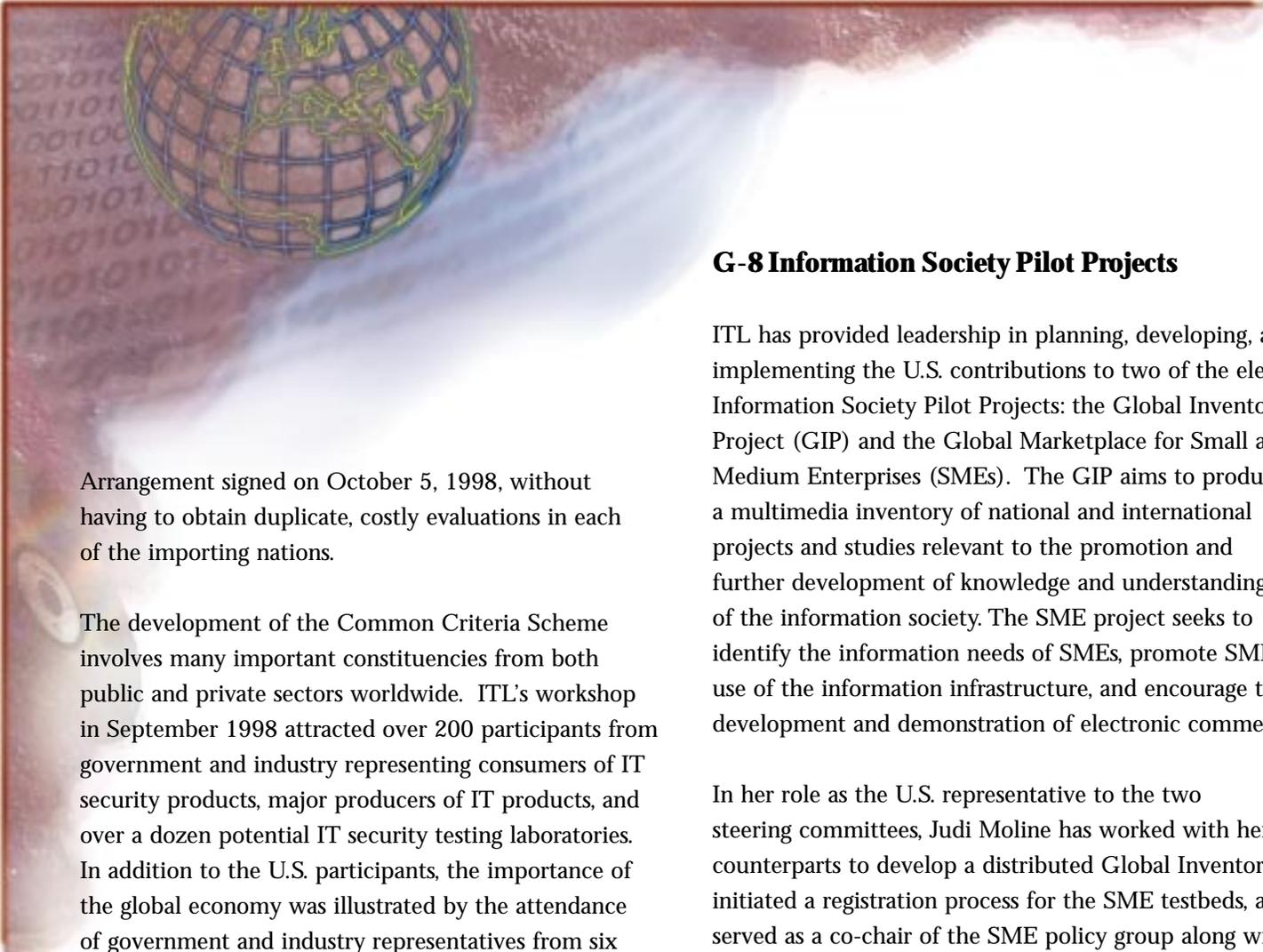
ITL and Chilsung Seo, Korea Telecom, developed the conformance test suite for the DSMCC-UU (Digital Storage Media Command and Control - User to User) protocol ISO 13818-6, which was included in the final Committee Draft of Part 10 of the MPEG2 standard (ISO/IEC JTC1/SC29 WG11 13818-10) in its 41st meeting in Fribourg, Switzerland.

Classification Society of North America

David Banks, Statistical Engineering Division, was elected in FY 1998 as the incoming chair of the Classification Society of North America (CSNA) and will serve from 2000-2002. Established in 1956, the CSNA promotes statistical research in cluster analysis and related fields, and publishes the Journal of Classification. The CSNA Web site can be found at <http://www.pitt.edu/~csna/csna.html>.

Common Criteria (CC)

As part of the National Information Assurance Partnership (NIAP), ITL is developing a Common Criteria Evaluation and Validation Scheme for Information Technology (IT) Security. The scheme will provide an organizational structure and framework for private sector testing laboratories to conduct security evaluations of IT products using the Common Criteria, an emerging ISO standard (FCD 15408). Results from the IT security evaluations will be validated by NIAP. Upon successful completion of the security evaluations and follow-on validations, NIAP will issue Common Criteria certificates that will be recognized under the Arrangement. U.S. manufacturers will now be able to sell their evaluated, security-enhanced IT products to any of the participants (e.g., Canada, France, Germany, and the United Kingdom) in the Mutual Recognition



Arrangement signed on October 5, 1998, without having to obtain duplicate, costly evaluations in each of the importing nations.

The development of the Common Criteria Scheme involves many important constituencies from both public and private sectors worldwide. ITL's workshop in September 1998 attracted over 200 participants from government and industry representing consumers of IT security products, major producers of IT products, and over a dozen potential IT security testing laboratories. In addition to the U.S. participants, the importance of the global economy was illustrated by the attendance of government and industry representatives from six foreign countries. The NIAP Web site is <http://niap.nist.gov/schemeCC.html>.

Cryptographic Module Validation

ITL and the Communications Security Establishment of the Government of Canada collaborated on the development of the Cryptographic Module Validation Program, which has been operational since July 1995. At the end of FY 1998, 26 hardware cryptomodules and 3 software cryptographic modules have been validated. 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. ITL and CSE also co-sponsored a conference in May 1998 on "Assuring Cryptographic Security: Development, Validation, and Use of FIPS 140-1 Compliant Products."

G-8 Information Society Pilot Projects

ITL has provided leadership in planning, developing, and implementing the U.S. contributions to two of the eleven Information Society Pilot Projects: the Global Inventory Project (GIP) and the Global Marketplace for Small and Medium Enterprises (SMEs). The GIP aims to produce a multimedia inventory of national and international projects and studies relevant to the promotion and further development of knowledge and understanding of the information society. 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 commerce.

In her role as the U.S. representative to the two steering committees, Judi Moline has worked with her counterparts to develop a distributed Global Inventory, initiated a registration process for the SME testbeds, and served as a co-chair of the SME policy group along with the Japanese and European Commission designates. ITL has kept the Global Marketplace Project focused on the SMEs through the testbed project reports. The stated key objectives of the G8 Pilot Projects in general are to support international consensus on common principles governing the need for access to networks and applications and their interoperability and to help create markets for new products and services. The Web site is <http://nii.nist.gov>.

International Federation for Information Processing (IFIP)

ITL participates in the IFIP Working Group on Numerical Software (WG 2.5), which is part of the IFIP Technical Committee on Programming Languages (TC 2). Ronald Boisvert, a member of WG 2.5, made a presentation entitled "Developing Numerical Libraries in Java" to the IFIP WG 2.5 meeting in May 1998 in Patras,

Greece, in order to elicit support from the international community for the Numerics Working Group of the Java Grande Forum. The Numerics Working Group is chartered to be the voice of the community on changes to Java which would make it suitable for numeric-intensive applications, as well as a center of coordination for the development of community-supported class libraries and interfaces for core numerical computations. The Web site is <http://math.nist.gov/javanumerics>.

Japan's Electrotechnical Laboratory

The Mathematical and Computational Sciences Division is collaborating with Japan's Electrotechnical Laboratory (ETL) on the design of high performance mathematical software for numerical linear algebra. As part of this work, ETL developed and maintains a mirror Web site for the Matrix Market in Asia, including a visual database of large sparse matrices from industrial applications, while NIST is incorporating interactive matrix generation software from ETL into the Matrix Market.

Russian Academy of Sciences

With funding from the Civilian Research and Development Foundation (CRDF), Daniel Lozier, Mathematical and Computational Sciences Division, and Dr. Yuri Rappoport, Russian Academy of Sciences, are collaborating in developing new mathematical algorithms and software for computing special functions with complex arguments and parameters. Numerical methods based on asymptotic expansions and differential equations have been shown to be effective for Airy functions and are being extended to Bessel functions of pure imaginary order. (The former functions are central in the theory and application of uniform asymptotics, and the latter arise in certain integral transforms.) Besides

being very general, this numerical approach is applicable for computing to high precision over broad ranges, and therefore is especially appropriate for constructing software tests. An addendum to the two-year CRDF grant supported a two-month visit to Moscow in FY 1998 by postdoctoral fellow Bruce Fabijonas to collaborate with Yuri Rappoport on mathematical and computational details.

Swedish Academy of Engineering Sciences

On September 11, 1998, ITL welcomed a delegation of 14 scientists from the Royal Swedish Academy of Engineering Sciences. The delegation selected ITL as one of the high-tech laboratories on the East Coast that they wanted to visit. The Swedish visitors expressed interest in new and exciting information technology subjects such as virtual reality and artificial intelligence. ITL presentations during the visit focused on human language technology, virtual reality in manufacturing, image recognition, role based access control, trends in distributed learning, the instructional management project of EDUCAUSE/ITL, mobile code and related agents, and Y2K work at NIST. ■



Staff Recognition

Department of Commerce (DoC) 1998 Medal Awards and NIST Awards

Kathleen M. Roberts, Office of the Director, received the DoC Bronze Medal for leadership in and dedication to the mission of the Information Technology Laboratory. Kenneth Robert Glenn, Advanced Network Technologies Division, was recognized with the DoC Bronze Medal for scientific and engineering achievement in the research, development, standardization, and commercialization of Internet security technology.

Chih-Ming (Jack) Wang, Statistical Engineering Division, received a DoC Bronze Medal Group Award with four NIST colleagues for developing measurement techniques and standards to provide industry with means to accurately characterize optical polarization parameters.

Timothy Burns, Mathematical and Computational Sciences Division, received a DoC Bronze Medal Group Award with a NIST colleague for their outstanding contributions to the theoretical and experimental understanding of chip dynamics in high-speed machining processes, which are of increasing importance in manufacturing.

Victor McCrary, High Performance Systems and Services Division, was honored with NIST's Equal Employment Opportunity Award for excellence in encouraging minorities and others to excel at NIST.

Lisa Marie Gill, Statistical Engineering Division, received the Measurement Services Award for her contributions to the Standard Reference Materials Program, where she worked with scientists and managers to effectively deliver NIST measurement services.

Walter S. Liggett, Jr., Information Access and User Interfaces Division, was awarded NIST's Chemical Science and Technology Laboratory (CSTL) Technical Achievement Award for contributions which resulted in the issuance of SRM 2806 Medium Test Dust (MTD) in Hydraulic Fluid and RMs 8631 Medium Test Dust and 8632 Ultra-Fine Test Dust.



W. Liggett



F. Podio



A. Rukhin and M. Vangel



External Staff Recognition

The Federal Laboratory Consortium (FLC) selected the team of David Ferraiolo, Richard Kuhn, John Barkley, Anthony Cincotta, all of ITL, Serban Gavrilla, VDG, and Janet Cugini, Citicorp, to receive an Award for Excellence in Technology Transfer for 1998 for their work in Role Based Access Control (RBAC). The award recognizes Federal Laboratory employees who have done an outstanding job of transferring technology developed in the laboratory to partners in government agencies as well as the private sector.

G.W. (Pete) Stewart, a faculty appointee in ITL's Mathematical and Computational Sciences Division, received the F. L. Bauer prize from the Technical University of Munich. The award honors Fritz Bauer, a computer scientist and numerical analyst who was a major player in establishing computer science as a discipline in Germany. Stewart, a Professor of Computer Science at the University of Maryland, was recognized for his lifetime achievements in the field of numerical linear algebra.

The American Statistical Association (ASA) presented the W. J. Youden Award in Interlaboratory Testing to Mark Vangel, a mathematical statistician in ITL's Statistical Engineering Division, and Andrew Rukhin, Department of Mathematics and Statistics, University of Maryland, Baltimore County, who holds a faculty appointment in ITL. Vangel and Rukhin were recognized for a pair of related papers that make major contributions to the statistical methodology for planning and analysis of interlaboratory experiments.

The Association for Information and Image Management International (AIIM) named Fernando Podio, High Performance Systems and Services Division, as "Laureate of Information Technologies in Electronic Document Image Management" for significant achievement in the area of electronic document image management, education, and industry experience gained through active involvement with AIIM. AIIM International is the leading global association bringing together information management professionals and providers of digital document technologies. ■

Services to Staff and Public

In FY 1998, ITL provided a wide range of supporting services to the NIST staff and the public, including:

Scientific Collaboration

ITL collaborated with other NIST organizational units (OUs) on many areas of mutual interest, including the following:

Flat Panel Display Interface

John Roberts, High Performance Systems and Services Division, and George Jones, Electronics and Electrical Engineering Laboratory, participated in laboratory verification of an analog display signal quality standard. ITL's contribution involved instrumentation and signal protocols.

LabVIEW Software

ITL negotiated an agreement with National Instruments which provides the NIST technical staff access to the LabVIEW Full Development System. LabVIEW is a graphical software system for developing high-performance scientific and engineering applications. NIST has more than 70 users of LabVIEW, one of the

major data acquisition software packages used by industry and in a number of NIST research and development projects.

Micromagnetic Modeling

ITL, the Materials Science and Engineering Laboratory, and the Electronics and Electrical Engineering Laboratory led a regional workshop of the Micromagnetic Modeling Activity Group (muMAG) at the NIST-Boulder Laboratories in August 1998. MuMAG is an organization of industrial, government and academic researchers investigating fundamental issues in micromagnetic modeling.

Next Generation Internet (NGI)

ITL, the Manufacturing Engineering Laboratory, and the Building and Fire Research Laboratory worked together to demonstrate NIST's efforts in the NGI initiative at the March 1998 "Netamorphosis" event hosted by the White House Office of Science and Technology and the National Economic Council. NIST joined other federal agencies in demonstrating advanced applications and new networking technology that are being developed through the NGI program.

Nonlinear Dynamics Models for High-Speed Machining

Timothy Burns, Mathematical and Computational Sciences Division, worked with Matthew Davies, Automated Production Technology Division, Manufacturing Engineering Laboratory, to develop a new approach to modeling some high-speed machining processes that has the potential to predict the onset of discontinuous chip formation in manufacturing processes.



C. Spangler expands the network backup service to include more desktop systems. The current ADSM (network backup software) configuration supports over 350 servers and stations using the STK robotic tape subsystem pictured. The additional system is capable of supporting 250 new clients and will also utilize the STK SILO tape storage.

OOF System for Simulating Measurements of Material Microstructure

ITL's Mathematical and Computational Sciences Division and the Materials Science and Engineering Laboratory's Ceramics Division and Center for Theoretical and Computational Materials Science released version 1.0 of OOF in September 1998. OOF is a finite-element program for analyzing material microstructures and conducting simulated physical property measurements on those microstructures. OOF allows materials scientists to determine the influence of microstructure on a material's macroscopic properties through an easy-to-use graphical interface.

Optical Absorption Software

As part of ITL's series of collaborations with other OUs on custom scalable parallel software, Judy Devaney, High Performance Systems and Services Division, delivered Optical Absorption parallel code and associated documentation ready for production use to the Physics Laboratory. ITL also demonstrated the use of WebSubmit, an advanced Intranet application tool.

Time Synchronization for Distributed Computing

Alan Mink, High Performance Systems and Services Division, worked with the Physics Laboratory (PL) to investigate distributed software time synchronization algorithms targeted to achieve one microsecond precision for the synchronization service on the Internet that PL administers. NIST hardware support instrumentation

was used to evaluate the precision achieved and to identify the impediments encountered. These low-cost techniques and guidelines can then be transferred to industry.

Computing Support to the NIST Staff

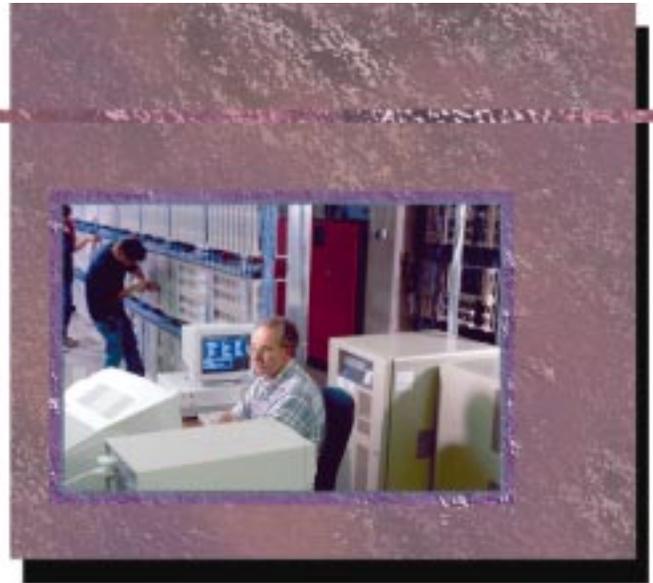
ITL provided comprehensive support to NIST's scientific and administrative computing customers, including the following:

- an easy-to-use, robust, secure, distributed heterogeneous environment with support for desktop systems and workstations, network capabilities, information services, and access to external and mobile users;
- common computing environments, information access tools, software development tools, and specialized applications software;
- site-wide hardware maintenance for standardized desktop systems and workstations and site-wide software licensing;
- maintenance and repositories for standardized platforms and applications;
- large-scale testbeds, advanced prototypes, and reliable systems as part of the continuous improvement in scope and quality of service; and
- the NIST scientific computing system, networking, and telecommunications support.

R. Schaefer installs the operating system on the 24 CPU, 24 gigabyte memory, SGI Origin, the next phase in the continuing upgrade and enhancement of the NIST scientific computing resources. The system will provide a robust memory configuration in a SMP environment.



H. Fogle installs NIST's new Siemens telephone switch.



Selected Conferences, Workshops, and Training Courses

11th Federal Information Systems Security
Educators' Association (FISSEA) Conference

20th National Information Systems Security Conference

Display Forum '97

Federal Computer Incident Response
Capability (FedCIRC) Conference

First Advanced Encryption Standard (AES)
Candidate Conference

Fingerprint Data Interchange Workshop

Formal Methods in Software Development Tutorial

Improving Product and Process Design
Using Experiment Design

Mobile Agents and Security

Modeling and Simulation

NIST LabVIEW Users' Group

NIST Microsoft Access Users' Group

NIST Windows NT Administrators' Group

North American ISDN Users' Forum (NIUF)

Performance Evaluation of Hybrid Fiber
Coaxial (HFC) Network Protocols

Personal Identification from Mugshot Ear Images

Role of Photonics in Information Technology

Sixth Text REtrieval Conference (TREC)

Statistical Uncertainty: Classical and Bayesian Methods

Teaching Computers to Recognize Patterns

Training in Synchronize, Eudora, MS Word
and other NIST-wide applications

Tutorial on Hypothesis Testing

Usability Testing Results as Procurement
Criteria for Software

Workshop on Assuring Cryptographic Security

Workshop on FIPS 140-1

Workshop on Role Based Access Control (RBAC)

WWW Design and Development

ITL publishes a variety of publications, newsletters,
bulletins, and documents online. The Web site is
<http://www.itl.nist.gov/lab/csl-pubs.htm>. A link to
information about FY 1998 ITL staff publications
can be found at this Web site. ■

For more information, contact:

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

Telephone: (301) 975-2900

Facsimile: (301) 840-1357

Email: itlab@nist.gov

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

