AN ASSESSMENT OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INFORMATION TECHNOLOGY LABORATORY

FISCAL YEAR 2007

Panel on Information Technology

Laboratory Assessments Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS   500 Fifth Street, N.W.   Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the board responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. SB134106Z0011 between the National Academy of Sciences and the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the agency that provided support for the project.

Copies of this report are available from

Laboratory Assessments Board
Division on Engineering and Physical Sciences
National Research Council
500 Fifth Street, N.W.
Washington, DC 20001

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

PANEL ON INFORMATION TECHNOLOGY

JEFFREY D. ULLMAN, Stanford University, *Chair*
RICHARD S. BAKALAR, IBM Corporation
JOHN M. CARROLL, Pennsylvania State University
STUART I. FELDMAN, Google Inc.
DAVID R. FERGUSON, Boeing Corporation (retired)
ERIC H. GROSSE, Google Inc.
CYNDI JUNG, NVidia Corporation
JAMES M. LANDWEHR, Avaya Laboratories
PATRICK D. LINCOLN, SRI International Corporation
STEVEN B. LIPNER, Microsoft Corporation
WILLIAM A. MASSEY, Princeton University
ALEXA T. McCRAY, Harvard Medical School
HILARIE K. ORMAN, Purple Streak, Inc.
DAVID W. SCOTT, Rice University
ALFRED Z. SPECTOR, Independent Consultant
HAL S. STERN, University of California, Irvine
STEPHEN A. VAVASIS, University of Waterloo, Ontario, Canada
JAMES L. WAYMAN, San Jose State University

Staff

JAMES P. McGEE, Director
ARUL MOZHI, Senior Program Officer
LIZA HAMILTON, Administrative Coordinator

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

C. William Gear, NEC Research Institute, Inc.,
Betsy L. Humphreys, National Institutes of Health,
Sanjit K. Mitra, University of Southern California,
Max D. Morris, Iowa State University, and
John McHugh, Dalhousie University, Halifax, Nova Scotia.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Alton Slay, Warrenton, Virginia. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Summary

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) has been assessed by a panel of experts appointed by the National Research Council (NRC). The panel visited the six divisions of the Laboratory and reviewed their activities. The scope of the assessment included the following four criteria: (1) the degree to which the laboratory addressed national priorities; (2) the degree to which the programs were well motivated with respect to goals, innovation, definition of success, impact, dissemination to end user, and cost and timelines; (3) the technical merit of the programs; and (4) the adequacy of the facilities, equipment, and human resources. Based on its assessment using these four criteria, the panel found that

1. Work at ITL is generally at or near the top of the peer group of information technology (IT) research activities at national laboratories.
2. ITL has activities that solve important problems for other NIST laboratories and other federal agencies, as well as activities that support industrial standards in IT.
3. The new “matrix” organization of crosscutting projects offers great opportunities but also poses serious risks.
4. ITL is likely to experience significant growth over the next 5 years, and it is necessary to plan for this growth carefully, including directions that will involve new kinds of scientists.
5. Of the existing activities, the Statistical Engineering Division is most in need of immediate enhancement of its capabilities.
6. ITL is experiencing problems securing funding to pay high-caliber IT professionals as well as professionals in scientific areas that are not traditional for NIST.
7. There are problems with the interaction between mandated or desirable research activities and the standard computer-security policies that are widely respected at NIST and similar organizations.

Charge to the Panel and Description of the Assessment Process

At the request of the National Institute of Standards and Technology (NIST), the National Academies, through its National Research Council (NRC), has since 1959 annually assembled panels of experts from academia, industry, medicine, and other scientific and engineering environments to assess the quality and effectiveness of the NIST measurements and standards laboratories, of which there are now eight,[1] as well as the adequacy of the laboratories' resources. In 2007 NIST requested that four of its laboratories be assessed: the Information Technology Laboratory (ITL), the Chemical Science and Technology Laboratory, the Electronics and Electrical Engineering Laboratory, and the NIST Center for Neutron Research. Each laboratory was assessed by a separate panel of experts, and the findings of each panel are summarized in separate reports. This report summarizes the findings of the Panel on Information Technology.

NIST requested that the panel consider the following criteria as part of its assessment:

1. The degree to which the Laboratory programs in measurement science, standards, and technology address national priorities.
2. The degree to which the Laboratory programs in measurement science, standards, and technology are well motivated with regard to the following questions:
    a. What is the program trying to accomplish?
    b. What is innovative or different, as compared to efforts at other institutions, about the program's approach that will lead to success?
    c. Is success well defined?
    d. What will be the impact of success?
    e. How will success be disseminated to end users?
    f. How much will success cost, and how long will it take?
3. The technical merit of the Laboratory programs relative to the current state of the art worldwide.
4. Insofar as they affect the quality of the technical programs, the adequacy of the Laboratories' facilities, equipment, and human resources.

To accomplish the assessment, the NRC appointed a panel of 18 volunteers whose expertise matched that of the work performed by the ITL staff. The panel members were also assigned to six subgroups whose expertise matched that of the work performed by staff in the six divisions in ITL: Mathematical and Computational Sciences, Advanced Network Technologies, Computer Security, Information Access, Software Diagnostics and Conformance Testing, and Statistical Engineering. These subgroups of the panel separately visited ITL facilities for 1 or 2 days, during which they attended presentations,

[1] The eight NIST laboratories are the Building and Fire Research Laboratory, the Chemical Science and Technology Laboratory, the Electronics and Electrical Engineering Laboratory, the Information Technology Laboratory, the Manufacturing Engineering Laboratory, the Materials Science and Engineering Laboratory, the NIST Center for Neutron Research, and the Physics Laboratory.

tours, demonstrations, and interactive sessions with ITL staff. Subsequently, the entire panel assembled for 1.5 days, during which they attended overview presentations by ITL management and interactive sessions with ITL managers; the panel also met at this time in a closed session to deliberate its findings and to define the contents of this assessment report.

The panel's approach to the assessment relied upon the experience, technical knowledge, and expertise of its members, whose backgrounds were carefully matched to the technical areas within which the ITL activities are conducted. The panel reviewed selected examples of the standards and measurements activities and the technological research presented by the ITL; it was not possible to review the ITL programs and projects exhaustively. The panel's goal was to identify and report salient examples of accomplishments and opportunities for further improvement with respect to the technical merit of the ITL work, its perceived relevance to NIST's own definition of its mission in support of national priorities, and apparent specific elements of the ITL's resource infrastructure that is intended to support the technical work. These highlighted examples, for each ITL division, are intended to collectively portray an overall impression of the laboratory while preserving useful mention of suggestions specific to projects and programs that the panel considered to be of special note within the set of those examined. The assessment is currently scheduled to be repeated biennially; while the panel applied a largely qualitative rather than quantitative approach to the assessment, it is possible that future assessments will be informed by further consideration of various analytical methods that can be applied.

This report is organized in two parts. The first part discusses issues that apply broadly to several or all of the divisions or to ITL as a whole. The second part presents observations specific to each ITL division. The comments in this report are not intended to exhaustively address each program within ITL; rather, this report identifies key issues and salient programs and projects relevant to those issues.

General Assessment of the Information Technology Laboratory

A central part of the charge to the panel was to assess the quality of the work being done at ITL. The panel found that in general the appropriate peer group for this quality assessment was the U.S. national laboratories. The work at ITL generally ranks at or near the top of the work being done by peer institutions. There are some exceptions, principally cases where another laboratory has strong motivation to develop in a specialty area (e.g., laboratories concerned with nuclear weapons research have developed outstanding capabilities in high-performance computing).

RESEARCH STRATEGIES

This section identifies several impressive approaches to research at ITL. These approaches are quite innovative and in many cases unique to NIST.

Community Building

ITL has a long tradition of promoting research by serving as an honest broker for competitions. ITL scientists work very hard to learn the goals of a research community, and they present that community with appropriate challenges in the form of data, metrics, tasks, and evaluation protocols by which the community can test the performance of their system. Often, these challenges are offered in an annual competition. A repeatable methodology has evolved for involving the community, measuring performance, refining the challenges, and making the test data public after the fact, allowing new teams to join the community.

The original competition of this class is the ongoing challenge of speech recognition. ITL now also offers competitions in information retrieval, cryptography, face recognition, and language translation, for example. Several instances of this process have been created for external research agencies, which find the methodology to be an important tool for driving research.

Interoperability Testing

Making complex software systems interoperate is a difficult challenge. Thus, another important theme of research at ITL is the evaluation of commercial products for the ability of the results of one to be consumed by another. Examples include the US-Visit program, XML validation, and cryptographic device validation.

The US-Visit program uses devices that record fingerprints and compare them with their supposed matches. Two devices may not produce the same electronic representation of the same finger, even though each device conforms to the standard for representation. When the differences are inherent in the design of the device, it becomes impossible for the two devices to be used on the same person, because the probability of false negative becomes too high.

There is an ITL effort to specify best practices for defining and using the XML

Schema. ITL staff have written documents and tools to help assure that schema are well formed and that software processing the XML conforms to specifications (through published examples). The work also addresses schema reusability by developing guidelines for meta tools that control the naming and design of schema.

Cryptographic device validation is a mature initiative for accrediting laboratories that test cryptographic hardware and software. This process ensures that laboratories implement algorithms correctly and that they protect sensitive information, such as keying material, according to best practices. ITL provides testing software to the laboratories and defines the testing interface to implementors, streamlining both the testing process and the confidence in the results.

External Collaborations

The impact of ITL's work with external agencies can be found across the laboratory. There are some good collaborations, both with other laboratories at NIST and with external agencies. In the latter case, ITL staff are often supported by contracts to perform necessary work. In general, the contracted tasks are appropriate to the overall NIST mission and often enhance the overall research capabilities of ITL.

There are, for instance, external collaborations on health care with the Department of Health and Human Services, the Integrating the Healthcare Enterprise project, and the American Telemedicine Association. There is work on radiation detection for the Department of Homeland Security and work on speech processing for the National Security Agency.

The Boulder group of ITL's Statistical Engineering Division (SED) works with colleagues at the NIST Center for Neutron Research on a project involving the imaging of hydrogen fuel cells. Water management in the fuel cells, where water is a by-product, is crucial, and neutron imaging is a uniquely good way to monitor water in the operating fuel cell. Statisticians have worked on strategies for improved image processing to assist in monitoring the water.

SED personnel were approached by the Department of Homeland Security just before a radiation-detector evaluation experiment comparing different vendors was to be conducted at the Department of Energy's Nevada Test Site. The evaluation had already been designed, and SED was originally approached to assist only with data analysis. The resulting report was adopted as the sole analytic input to the vendor selection process. In addition, the work of SED was valued so highly that the division has now been incorporated into the design and analysis for subsequent phases of the project.

OPPORTUNITIES

ITL is beginning several interesting directions for research, which ITL management should promote and grow. A number of the opportunities described by ITL are identified below.

Medical Informatics

There is a huge national challenge in making health systems interoperate. These systems include patient medical records and telemedicine. The problems are addressable by the traditional strengths of ITL—they will almost always involve the creation of standards and the validation of interoperability among different commercial systems.

ITL has made some effort in these directions, such as HL7 message conformance and telemedicine standards. However, there is much more to be done. ITL should expand this effort, including establishing the links needed with other agencies and other stakeholders, creating relevant projects, and organizing interdisciplinary teams to execute the projects. As a first step, it should develop a strategic plan for research in this area and should augment its leadership capabilities here. Special attention should be given to identifying people in biomedical informatics who could provide such leadership and/or scientific capabilities. Credible performance in this area may require M.D.s in leadership positions.

Metrology

Metrology science is the bread and butter of NIST. There are a number of ways in which the work of ITL creates new challenges in this area, and ITL staff should tackle them. In a number of recent activities, standards or evaluation procedures involve a human in the loop—that is, a human has to examine each submission and make a subjective decision as to its quality. In some cases this is analogous to defining the weight of a kilogram by what an expert on weights *thinks* should be a kilogram. While there may be cases where nothing better can be done to eliminate subjective judgment, ITL staff should think carefully about these procedures. Removing human judgment from an evaluation, even partially, can have two advantages: It usually reduces cost, and it avoids the arguments that arise when there are subjective evaluations. A good example is the Mathematical and Computational Sciences Division's recent algorithms work, which replaced equipment adjustments previously done by forensic laboratory technicians. ITL should also further develop measures for correct translation among natural languages. As for another example, the routine way to evaluate translation of a natural language is to give each translation to a human to evaluate. This process is expensive and does not scale. Another approach, which ITL is looking into, involves a human setting down criteria for correctness of the translation of a small passage, and then having a machine check the criteria without having to consult the human on every submission.

Standards are generally assumed to be beneficial, but the proof for this assumption is sometimes lacking. As an example, the Federal Information Security Management Act (FISMA) has been applied broadly, but its benefits are not known. ITL should consider investigating the effects of standards and should develop a broadly applicable methodology for such investigations.

Statistics

There has been attrition in SED over the past 2 years, and a new division head has been appointed. Like the Mathematical and Computational Sciences Division in ITL, SED's primary focus is on collaborative research with other groups at NIST, primarily outside ITL.

While growth is justified in many of ITL's divisions, there is an especially urgent need to expand activities in statistical engineering. Most significantly, there are a number of subdisciplines of modern statistics where in-house expertise is lacking and practitioners of these arts are needed.

Secure Networking

There is an opportunity to serve ITL's own needs for secure access to external computing resources and at the same time do research in an interesting new direction. The section on computing infrastructure, below, discusses this opportunity in further detail.

PLANNING FOR GROWTH

NIST's budget is projected to double over the next 5 years. Even if that projection is not realized, there will undoubtedly be substantial opportunity for growth in the near future. ITL should be prepared with a roadmap for that growth.

Demographics

The average age of laboratory members is rather high, and the change over the past years has not been good. The average age in one division rose by 4.1 years over the past 4 years. The age distribution shows a dearth of 30- and 40-year-olds, the age at which scientists and engineers tend to mature and increase their effectiveness.

Temporary Versus Permanent Hires

ITL should identify the areas in which it would be most useful to grow and should develop a strategic plan for such growth. The plan needs to take into account long-term versus temporary hires. There is an advantage to being able to hire someone for a limited time and then turn to someone else as priorities change. Yet competition with industry is severe, and talented people are unlikely to accept the risk of a short-term appointment in addition to a salary structure that cannot compete with what industry offers.

A significant fraction of the ITL budget comes from other federal agencies. Some of these arrangements have proved to be reliable over the years, while others soon disappear. Giving a potential hire the impression that his or her position is temporary and that he or she would have to compete against all comers for a permanent position would be sufficiently negative to deter top people. It is encouraging that none of the divisions reported such an event and that it is apparently possible to avoid competing a position when converting temporary staff to permanent. However, the risks are real, and ITL should look carefully at how temporary positions are used.

Hiring in Nontraditional Areas

Some interesting directions are best served by nontraditional hires. In some observed cases the appropriate background could be different from that of the stereotypical hard scientist (e.g., a physicist or chemist). For example, assessing the usability of voting machines requires thinking carefully not only about people with recognized disabilities (e.g., blindness) but also about people with other limitations (e.g., arthritis). A physical therapist or other relevant health-care professional could add an important perspective to this kind of evaluation. As another example, the realization that a translator of natural languages would be an essential part of a team for evaluating machine-translation software proved to be problematic because at NIST translators are classified as office staff rather than scientists. ITL management should consider hiring in nontraditional areas when appropriate to the mission, and NIST management should try to remove impediments to such hires.

Status of the Information Technology Staff

The data from ITL suggest that the laboratory has a rather small proportion of the senior scientific and technical positions ("SES" equivalent) that have been allocated to NIST. One reason for the disparity may be the awards garnered by scientists in other NIST laboratories. There are Nobel winners among the scientists of NIST; the panel is not aware of analogous ITL staff (e.g., Turing award winners or Fields medalists). On the other hand, information technology is vital to U.S. competitiveness. More than a third of all new jobs created in the United States in recent years are in information technology. Moreover, these jobs tend to be "good" jobs. In his book *The World Is Flat* Thomas Friedman reminds us that the wealth of a nation is today determined by the strength of its IT. Attracting more top people to ITL, given the areas it covers, makes sense in the light of this reminder.

THE RESEARCH CULTURE

There are two ways, discussed next, in which the reputation of ITL can be enhanced.

Marketing

There is no one model for outreach that applies to all the divisions of ITL, and it may be appropriate for different divisions to market their work in somewhat different ways. However, in general there are two ways to have influence: through publications and through outreach—formal and informal interaction with other groups. Some divisions publish regularly; some do not. Some have external visibility; others do not. Both modes of enhancing external visibility should be considered seriously by every division. If a division is not doing both, then management should at least understand why not.

Seeking Research Opportunities

It is important that a large proportion of the scientific and engineering staff be alert to new opportunities. Ideally, many on the ITL staff would be searching actively for the next important problem to work on, and certainly some are. However, more ITL staff should be doing so, and management should facilitate a more adventuresome approach to research.

THE PROJECT/PROGRAM MATRIX

A recent ITL innovation is the establishment of crosscutting projects that have their own leadership and budgets. The creation of interdisciplinary projects is a good thing for ITL. Yet, things can go wrong if their introduction and management are not handled carefully. The plan for matrix management at ITL is not likely to succeed unless there is more enthusiasm for the plan among the staff. The following is an outline of some of the risks:

- It is hard to will research projects with impact into existence. A successful research project requires buy-in—a belief by the participants in the importance of the project. Ideally, the project is created by the staff of the project itself.
- It is necessary to find leaders who are enthusiastic advocates for the project. They need to be able to inspire people on the team and to support the shared vision with management above. Project leaders should have strong technical or scientific credentials.
- If policies are not made very clear, there will be reason for staff to worry about how they fit in. Staff may be concerned about whether they will be evaluated by their project leader, their division chief, or both. They may wonder whether everyone will eventually be part of a project or whether those who want to will be able to continue working in their own preferred discipline.
- The funding model may distort operations. For example, the initial budget for the ITL projects came from an approximately equal “tax” on each of the divisions. However, the current projects are not now, and may never be, equally suitable for members of all of the divisions. As a result, there will be unintended winners and losers.

There is an opportunity to use the anticipated growth to bring in leaders and key staff for some exciting new projects. ITL management should communicate more with the staff to identify and allay some of the concerns that have been raised and to provide assurances that their work and status do not depend on whether or not they are participating in a project.

While the stability of government programs should not depend on the personnel assigned to them, maintenance of a stable group of mature professionals is necessary for the efficient execution of complicated technical challenges. When converting to a matrix management structure, ITL should avoid disrupting the established challenge problems of the Information Access Division and seek to keep the experienced expert staff in place.

COMPUTING INFRASTRUCTURE

The equipment resources are adequate to serve the needs of the research. However, there is a limitation of another kind. For obvious and valid reasons, the Department of Commerce has instituted strong new controls over computer and Internet use to minimize the risk of intrusion or other attacks on its computer systems and data. The risks of circumventing or ignoring these controls are high.

However, the new policies have created some serious impediments to research at NIST, and at ITL in particular. One example illustrates the problem: The Advanced Network Technologies Division has been mandated by Congress to provide a roadmap whereby the entire U.S. government will adapt to IPv6 (Internet Protocol Version 6), yet it has been unable to gain access to an IPv6 experimental network. Such networks exist outside NIST and could be used, but not without violating policy.

The problem described is not unique to NIST and will become more widespread. Moreover, the issues surrounding how to work around the problem largely involve standards. Therefore ITL itself should undertake the research necessary to provide a next generation of security standards that will facilitate rather than inhibit the activities that a research organization needs to conduct.

Assessments of Laboratory Divisions

MATHEMATICAL AND COMPUTATIONAL SCIENCES DIVISION

National and Agency Priorities

The Mathematical and Computational Sciences Division (MCSD) has a well-formulated view of the way it contributes to national priorities by advancing science and industrial innovation, and individual contributors understand how their work fits with the goals of NIST. In particular, the teams understand the importance of simulation-based engineering and how to deliver their technology to scientists and practitioners, inside and outside NIST, who are the ultimate users. Two projects clearly address national priorities:

- Numerical Optimization of Complex Instrumentation uses mathematical methods to determine appropriate settings for spectroscopy instruments, enabling less subjective forensic analysis. The work here has already improved standardization and repeatability of analyses, resulting in a more robust process.
- The OOF2 (Object-Oriented Finite Element Analysis) project on image-based finite-element analysis of material microstructures has evidently met its goal of system portability, based on what enthusiastic users say. It is contributing to advances in materials science, particularly the development of novel alloys.

MCSD staff have the scientific expertise required to make significant contributions to this technical thrust. Their research publications, numerous collaborations, and education level (72 percent hold Ph.D.'s) attest to their readiness to perform their mission.

Technical Merit

Researchers have plenty of collaborators, are well published, and participate in scientific conferences and workshops. Overall, the technical merit of the projects measures up to the current state of the art. The projects reviewed have well-defined end users and a clear idea of how they will succeed. Typical projects include these:

- Modeling of Rheological Properties of Suspensions uses up-to-date scientific computing methodology to help understand the properties of cement-based materials. The project is well connected to worldwide industry.
- The Digital Library of Mathematical Functions project cleverly chose contour-fitted grids to produce proper visualizations of special functions. Such attention to detail will contribute to a worthy modern successor to Abramowitz and Stegun's widely used *Handbook of Mathematical Functions*.
- Recent publications indicate that MCSD's work in quantum computing is of the highest caliber.

The technical merit of MCSD work is also recognized by scientific colleagues. A member of the staff won the prestigious Arthur S. Flemming Award given to young federal agency employees. Two members of MCSD are now fellows of the American Physical Society, and one was recently honored as a distinguished scientist by the Association for Computing Machinery (ACM).

Facilities and Staff

Facilities appear sufficient for the research activities. Most projects are doing well enough with existing computers; one project with greater needs was allocated a large amount of supercomputer time. MCSD's move from the adjunct campus to the main NIST campus will help collaboration. Individual researchers have adequate two-person offices. The work of MCSD requires tremendous individual concentration not usually attainable in multiperson offices, so if space constraints dictate a more compressed working environment, ITL management should support alternatives such as telecommuting part-time in order to preserve or even enhance the work environment.

Morale is reasonably high, and the staff are clearly confident of their research directions and management. They are not risk-averse in the sense that members are quite willing to forge partnerships outside ITL and outside NIST. ITL staff expressed some concern over hiring and budget shifts. Also, staff and management expressed a desire for more postdoctoral positions and are taking steps to obtain necessary resources; more postdoctoral hires would be good for MCSD. Lastly, ITL should plan carefully to develop program managers and successors for the division management.

INFORMATION ACCESS DIVISION

The Information Access Division (IAD) within ITL has many long-standing, externally funded challenge programs in speech, text, and image processing, aimed at improving national technical capabilities by enticing industry and academia to address problems of interest to the government. Three examples of such programs are the Text Retrieval Conference (TREC), the Language Recognition Evaluation (LRE), and the Face Recognition Vendor Test (FRVT). There are no other external programs of such depth and maturity, and these challenge programs attract a wide variety of international participants.

The other IAD challenge problems—Speech Recognition Evaluation, Spoken Term Detection, TREC Video, Document Understanding Conference, Fingerprint Minutiae Interoperability Exchange Test, Machine Translation Evaluation, and ACQUAINT—also have no peers. As a whole, they represent an important national asset.

These programs deserve to be fostered and protected. While the stability of government programs should not depend on the individuals assigned to them, a stable group of mature professionals must be maintained for the efficient execution of these complicated technical challenges. When converting to a matrix management structure, ITL should avoid disrupting the established IAD challenge programs and should seek to keep the expertise in place.

IAD has been asked to establish standards and evaluation programs for a number of human-centric technologies, such as voting machines, machine text translation, and content-based access methods. “Human-centric” means that humans are either part of the process or direct consumers of the machine output. The performance of such technologies must be assessed in the context of human cognition and physical capabilities. Standards development and evaluations, particularly of technical systems to be used by the public, such as voting systems, must be done with a focus on universal accessibility. (“Universal accessibility” is to be understood here in the broadest possible sense, including young, middle-aged, old; tall, short; left-/right-handed; and near-/far-sighted) Such evaluations require professionals with expertise outside the traditional ITL disciplines of mathematics, statistics, engineering, physics, and computer science. Recognizing this, IAD has been hiring and developing expertise in the social sciences, but it should prepare for even more staff growth in these areas. ITL should strive to remove barriers to hiring professionals outside the traditional mathematical and engineering sciences.

STATISTICAL ENGINEERING DIVISION

Addressing National Priorities

The SED research program plays a significant role in ITL’s work in support of national priorities. The division’s statistical metrology effort is a unique national resource. Its expertise on issues related to measurement, including novel work on Bayesian methods to combine information about both statistical and nonstatistical sources of error, is an important asset. In addition, SED personnel play a vital role in collaborative efforts with other NIST programs, helping those programs to address relevant national priorities—for example, a collaborative project with the NIST Center for Neutron Research supports development of hydrogen fuel cells. SED continues its long-standing vital contribution to NIST’s manufacture of standard reference materials (SRMs), with every SRM requiring SED validation. Finally, SED now plays a significant role in support of national needs expressed by other U.S. government departments and agencies. Noteworthy in this regard is an ongoing project for the Department of Homeland Security (jointly with personnel from the NIST Physics Laboratory) on evaluation of radiation detectors as part of the effort to protect the United States against nuclear terrorism.

Impact of Programs

The SED research program has a clearly identified mission that emphasizes (1) support and collaboration for NIST research efforts; (2) participation in international metrology efforts; (3) support for the NIST SRM program; (4) participation in projects for outside agencies; and (5) education and outreach to teach about uncertainty and to describe measurement work within NIST, including interdisciplinary collaborations with the physical sciences and assuming a leadership role in the international metrology community. Success in these efforts has a clear link to the national priorities being addressed by NIST to enhance industrial competitiveness.

Technical Merit

The statistical metrology research program is clearly state of the art. SED researchers publish regularly in international metrology journals and are among the leaders in international metrology efforts. One member of the staff was recently appointed as a permanent member of the primary international measurement group's committee that promotes statistical tools in measurement. SED has been recognized as the largest statistical team focusing on metrology. The collaborative research with other NIST laboratories is also making use of state-of-the-art statistical methodology and stands as a strong example of the potential for science-motivated collaborations to advance the development of statistical methodology. For example, SED's innovative work in experimental design ensures that NIST investments in experimentation and evaluation are as cost-effective as possible and will achieve the experimental goals. There is a need to expand SED's ability to bring state-of-the-art methodology to the many NIST projects that can use its support. This can be done by increasing the size of the division, as discussed below.

Facilities, Equipment, and Human Resources

The SED scientists appreciate the move that has colocated SED staff on the main NIST campus and note that it has important benefits for their collaborative work. The computational infrastructure is appropriate to the tasks the group performs.

SED needs additional human resources. The work being done is, as described above, significant and of high quality. SED staff reported that because of resource limitations they are being forced to choose among important projects. The SED scientists remain committed to their long-term mission of providing collaborative support for the projects across NIST. This has always been a difficult challenge (there are currently approximately 20 scientists in SED and more than 2,000 in NIST). New opportunities—for example, to develop standards for microarray studies in biology and to participate in crosscutting intra-ITL programs—are important to the national metrology effort and of interest to SED staff. However, the scientific staff at SED noted that participation in such efforts requires cutting back on their collaborative efforts with other NIST laboratories and with groups external to NIST. For example, the Metrology Group's focus on participating in international metrology efforts has meant that it has not been able to participate in some standards projects for the American Society for Testing and Materials. Additional staff are needed in SED and would represent an appropriate ITL investment.

ADVANCED NETWORK TECHNOLOGIES DIVISION

The Advanced Network Technologies Division (ANTD) contributes in a number of networking areas, all of which are of growing importance to the nation's competitive position in the world, as well as to the safety of its citizens. As part of securing the cyberspace infrastructure, it has stepped up to authoring the protocol standards that would make the naming and routing services of the Internet more secure and is pushing their deployment. It has responded to the needs of the various agencies of the U.S.

government by producing a guide for deploying IPv6, as it has been mandated to do by the Office of Management and Budget. In the ever-important area of communications between different public safety radio systems, ANTD has assisted the Department of Homeland Security with P25 intersystem specifications and hands-on interoperability testing (P25 is a suite of standards that specify the interfaces between the various components of a land mobile radio system).

In its mission of developing measures for new technologies, the division’s renowned work on quantum key distribution has produced a device for measuring the efficiency of any photon detector, and work with entangled photons is on the horizon. The broad area of complex information systems, a new program involving scientists from multiple divisions within ITL, has uncovered surprising causality between simple actions of network components and chaotic network events.

ANTD’s various wireless projects are timely for industry and the nation, addressing a mix of public safety and private sector concerns. Both the clever use of radio technologies for tracking and identifying people inside a building and the development of methods for rapid deployment of ad hoc wireless networks based on vector quantization of received signal strength build on the strong wireless expertise in this division.

The division could do even better work if it had access to certain external research networks connected independently of the NIST campus network for security reasons. The IPv6 work lacks credibility without having a network attachment to the worldwide interconnected networks running IPv6, and when the National Science Foundation’s (NSF’s) Global Environment for Network Innovations (GENI) project goes live (the goal of the GENI project is to increase the quality and quantity of experimental research outcomes and transitions in networking and distributed systems), NIST would be conspicuously absent without a link to it. This is an ongoing problem that needs to be solved.

Also, there are several opportunities for applying massive computing to some very important networking problems. For example, doing sufficiently accurate simulations of network behaviors, with enough breadth of experiment for statistical credibility, could benefit from orders of magnitude more computing than is currently available at NIST. Institutional commitments to internal investment as well as participation in the use of national resources could be most useful.

COMPUTER SECURITY DIVISION

NIST’s mandated role in support of FISMA requires significant effort and the development of many standards documents. FISMA was created as a way to protect federal information systems, but it also involves the creation by federal agencies of a great deal of documentation. The effectiveness of certification and accreditation processes such as those mandated by FISMA in bringing about effective security and protection is far from universally accepted by computer-security professionals. Although certification and accreditation processes play a significant role in computer security today, standards and guidelines should have their success firmly demonstrated. ITL has not demonstrated the success of its guidelines, and its customers may have reservations.

Cryptography

ITL is a respected leader in cryptography competitions, and its work in this area is first-rate. The NIST-led competition that resulted in the creation of the Advanced Encryption Standard (AES) is well respected. The Computer Security Division's (CSD's) Encryption Group merits a high level of support to ensure the continued success of ITL's cryptographic standards work.

One criticism is that NIST competitions have had shifting criteria for success. Competitors have sometimes lobbied for adding new criteria or valuing one criterion over another, and this lobbying introduces an additional dimension to the competition, one that is subjective and not as transparent as might be desirable. ITL is planning to conduct a competition for a new generation of cryptographic hash functions, and there should be clear criteria for the evaluation of candidate hash functions.

Research on quantum computing and its impact on cryptography is speculative. It is appropriate to conduct such research at NIST, which has qualified researchers investigating the area. Though it is not certain that quantum computing is possible, its success would require the development of new cryptographic standards.

Voting

Voting is a difficult area within which to develop standards, and NIST's impact may be minimal in this area. NIST is probably in a good position, however, to gather information about the multitude of ballot types and to develop a generic ballot description language.

Policy Machine

NIST has initiated a project in pursuit of a standardized access control mechanism, referred to as the Policy Machine (PM). The project takes a very generic approach to policy management, but the architecture seems to include a centralized decision-making component that is unnecessarily constraining. Project members insist that it could be decentralized with commonly used techniques, but this seems to ignore the fact that some decisions must be made locally (within a small administrative domain). It is not clear that this is an area amenable to standardization. Nonetheless, it is forward-looking research in an important area that might bear fruit. The Internet Engineering Task Force has some policy management efforts—for example, IPsec (Internet Protocol security) policy based on an extensive and detailed mapping of IPsec standards to management information bases—some companies build security policy management methods on Microsoft's access control mechanisms, and almost every security research conference includes a few papers on policy management. ITL's work should be more heavily tied in to this outside work.

Also, the personal identity verification (PIV) work would seem a natural fit for the application programming interfaces being developed for the PM. Tying together the authentication with the authorization would be a strong argument for the utility of the PM.

Personal Identity Verification

NIST is making important contributions to interoperability by standardizing the critical components of personal identity verifications (PIVs). There are a surprising number of critical components surrounding PIVs, and standardization of information transfer and compliance testing are good ideas. This is solid work at the core of ITL's competencies. The intent to investigate ontologies is a good idea that might bring some order to the impending chaos of identity methods. The efforts to support timely issuance are laudable.

ITL should be looking at privacy, though, including consideration of the consequences of requiring a large amount of personal information to be carried on physical tokens, stored on computers at many government installations, and/or handled by contractors. The radio frequency identification (RFID) work considers a plethora of government policies and recommendations for privacy.

Radio Frequency Identification

The testing for eavesdropping and jamming is important work. It includes cryptographic methods to protect RFID tags and the systems that read them, and this is a difficult problem. There are some research papers published in proceedings of conferences on topics like cryptographic hardware and embedded systems; ITL should make its presence in the area more noticeable through outside associations.

Security Testing and Metrics

The requirements of NIST's Federal Information Processing Standard 140 (FIPS-140, Security Requirements for Cryptographic Modules) are well respected by vendors of cryptographic systems. These standards are important for assurance in cryptography for U.S. and foreign systems. ITL's role in validating laboratories that test products for compliance is appropriate and well conducted. The standards do have a reputation for being somewhat daunting to newcomers, and vendors may delay the effort to achieve compliance until they can afford to hire a knowledgeable consultant.

Over 90 percent of first-time applicants fail because their documentation is inadequate. One might conclude that the standards do not adequately convey what is needed, and ITL should consider improving the explanations. A smaller percentage (approximately 30 percent) fail the algorithm testing. ITL provides a very good tool to the testing libraries for checking functionality. If that tool were also available to applicants, they could easily do their own functionality testing and spend less time interacting with the testing laboratory. ITL should publish the testing tool as an open source project.

Automated Combinatorial Testing

This work is largely repetitive of efforts conducted during the 1980s, and it is unlikely to lead to effective processes for assessing the security of real software systems. ITL should expand the work and try to apply it to mature NIST testing programs. In particular, the crypto-validation program is a potential customer. As an example, the digital signature validation implementation error that was discovered in 2006 may have been the sort of error that the combinatorial testing could have discovered. The encoding of a digital signature involves a small grammar with a length field as an element. Combinatorial testing applied to the grammar might have developed tests for proper encoding of the length, and this might have revealed the implementation error long before visual inspection finally did.

SOFTWARE DIAGNOSTICS AND CONFORMANCE TESTING DIVISION

Addressing National Priorities

Several of the Software Diagnostics and Compliance Testing (SDCT) division's programs address important national priorities. The Help America Vote Act of 2002 (voting support), XML standards, computer forensics, and health information technology projects are among the most notable. ITL's role in electronic voting is paramount for ensuring that new voting systems perform as they should. The SDCT division is providing support to the Election Assistance Commission's Technical Guidelines Development Committee and works with voting officials, voting system vendors, and academic researchers to better understand the critical issues and possible approaches. The excellent SDCT division work that furthered the success of XML-related standards clearly is beneficial to information technology, and the particular standards are likely to improve national economic efficiency by permitting the better integration of diverse processes. The computer forensics project supports law enforcement agencies, particularly the National Institute of Justice, in their investigations of computer-related crimes. The health information technology project gives ITL the opportunity to contribute to the national agenda by addressing one of the most pressing problems in health care technology today, namely, methods to ensure measurable, confidential, and secure exchange of pertinent health care information.

The Degree to Which Projects Are Well Motivated

SDCT projects are well defined. Each clearly states the problem and the approach to it. Once a project has achieved its goals, it is subject to sunsetting and transfer to an appropriate industry or agency partner. The XML technologies conformance testing project is such an example. The SDCT team developed a comprehensive set of test suites for XML, which has been widely recognized for its high quality. The work has had a broad national and international impact, and it serves as a model for other testing and conformance efforts, which are well placed within this division's portfolio. While the XML project has been a success and is properly being sunsetted, it is not obvious how such decisions are made for other projects and whether a formal technology transfer plan is in place in all cases. SDCT project work is well received by colleagues in the federal agencies with whom division staff interact. Staff regularly prepare technical reports, but the impact and visibility of their work would be enhanced by more extensive publication in the peer-reviewed literature.

Technical Merit of the Programs

The technical merit of SDCT division programs is high, and the projects are conducted by technically competent individuals. Several of the projects that could have a very high impact are briefly discussed here. The voting project has a good specification and testing plan, and SDCT division staff are working with the relevant stakeholders to assess and define the needs of a trustworthy electronic voting infrastructure. It was not clear whether the security needs have been fully defined, and some collaboration with the security group within ITL could be desirable.

The computer forensics project is the gold standard for enabling the exclusion of known packaged software from forensic analysis. That is, the signatures of many common pieces of software have been identified. However, in order to be fully successful, the project would need to scale to a much larger number of software packages and libraries, and it would need to include downloaded software, which accounts for most of the software purchased or upgraded today. Either significant growth or a plan for technology transfer might be considered for this project.

The computational grid project is addressing an important problem, but the experiments to date consider only networks of 1,000 or fewer machines. This project should consider the trend to larger grids.

The software assurance metrics and tool evaluation (SAMATE) project is also addressing an important problem and has catalyzed efforts elsewhere—for example, the National Vulnerability Database, Cigital, and Symantec—but to stay relevant, ITL must scale up the size of the software examples. Even if some tools are unable to handle the larger code snippets, ITL should lead the definition of benchmarks that would guide industry toward the problems of direct interest to increase overall assurance of future systems.

The health information technology project has made some good progress in outreach and visibility in important national health care standards organizations and multidisciplinary medical associations such as the American Telemedicine Association. SDCT division staff have taken on a leadership role in the Integrating Healthcare Enterprise (IHE), an external group that promotes the coordinated use of existing standards in health care. The potential impact of ITL’s work in formulating standards for health care information technology standards is great. ITL is well positioned to play an important role in these efforts, but it would be desirable to have a mid- to long-term program roadmap and strong health informatics leadership commensurate with this broad and complex opportunity.

Adequacy of SDCT Division Resources

The facilities, equipment, and human resources are adequate for the work performed by the SDCT division. Many of the projects in the division are externally mandated and funded with targeted dollars. One way to foster innovative investigator-initiated research might be to grant the division some percentage of unconstrained funding each year. These funds would be dispersed at the discretion of the senior management and could be used to jump-start a few fledgling projects.

One issue of concern is that the research equipment is subject to sometimes onerous information technology regulations that interfere with carrying out the research mission. Also, overall administrative overhead seems to be increasing, with multiple new forms and regulations burdening the relatively small administrative staff.

Conclusions

1. Work at ITL is generally at or near the top of the peer group of IT research at national laboratories.
2. ITL has activities that solve important problems for other NIST laboratories and other federal agencies, as well as activities that support industrial standards in IT.
3. The new “matrix” organization of crosscutting projects offers great opportunities but also poses serious risks.
4. ITL is likely to experience significant growth over the next 5 years, and it is necessary to plan for this growth carefully, including directions that will involve several new kinds of scientists.
5. Of the existing activities, the Statistical Engineering Division is most in need of immediate enhancement of its capabilities.
6. ITL is experiencing a problem securing funding to pay high-caliber IT professionals, as well as professionals in scientific areas that are not traditional for NIST.
7. There are problems with the interaction between mandated or desirable research activities and the standard computer-security policies that are widely respected at NIST and similar organizations.