# AN ASSESSMENT OF FOUR DIVISIONS OF THE INFORMATION TECHNOLOGY LABORATORY AT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

# FISCAL YEAR 2018

Panel on Review of the Information Technology Laboratory at the
National Institute of Standards and Technology

Committee on NIST Technical Programs

Laboratory Assessments Board

Division on Engineering and Physical Sciences

A Consensus Study Report of

*The National Academies of*
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
*Washington, DC*
**www.nap.edu**

**THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001**

This activity was supported by Contract No. SB134117CQ0017/18107 with the National Institute of Standards and Technology. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number-13: 978-0-309-48555-5
International Standard Book Number-10: 0-309-48555-X
Digital Object Identifier: https://doi.org/10.17226/25283

Copies of this report are available from

Laboratory Assessments Board
National Academies of Sciences, Engineering, and Medicine
500 Fifth Street, NW #928
Washington, DC 20001

This publication is available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

Suggested Citation: National Academies of Sciences, Engineering, and Medicine. 2018. *An Assessment of Four Divisions of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2018*. Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/25283.

*The National Academies of*
SCIENCES • ENGINEERING • MEDICINE

## PANEL ON REVIEW OF THE INFORMATION TECHNOLOCY LABORATORY AT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

CONSTANTINE GATSONIS, Brown University, *Chair*
ROBERT BLAKLEY, CitiGroup, Inc.
MATTHEW (MATT) BLAZE, University of Pennsylvania
FREDERICK R. CHANG, NAE,[1] Southern Methodist University
KWANG-CHENG CHEN, University of South Florida
PHILLIP COLELLA, NAS,[2] Lawrence Berkeley National Laboratory
JAMES H. CURRY, University of Colorado, Boulder
BRENDA L. DIETRICH, NAE, Cornell University
SEYMOUR E. GOODMAN, Georgia Institute of Technology
ERIC GROSSE, Independent Researcher, Los Altos, California
INDRANIL GUPTA, University of Illinois, Urbana-Champaign
HELENA HANDSCHUH, Rambus, Inc.
BRUCE A. HENDRICKSON, Lawrence Livermore National Laboratory
H.T. KUNG, NAE, Harvard University
STEVEN B. LIPNER, NAE, SAFECode
RADIA J. PERLMAN, NAE, Dell EMC
STEWART D. PERSONICK, NAE, New Jersey Institute of Technology (retired)
PADMA RAGHAVAN, Vanderbilt University
JOHN A. SMOLIN, IBM Corporation
EUGENE H. SPAFFORD, Purdue University
KAREN E. WILLCOX, Massachusetts Institute of Technology
MOE Z. WIN, Massachusetts Institute of Technologye
EDMUND YEH, Northeastern University

***Staff***

AZEB GETACHEW, Senior Program Assistant
LIZA HAMILTON, Associate Program Officer
EVA LABRE, Administrative Coordinator
JAMES P. McGEE, Director
MARTIN OFFUTT, Senior Program Officer

[1] Member, National Academy of Engineering.
[2] Member, National Academy of Sciences.

## COMMITTEE ON NIST TECHNICAL PROGRAMS

ELSA REICHMANIS, NAE, Georgia Institute of Technology, *Chair*
MICHAEL I. BASKES, NAE, Mississippi State University
LEWIS BRANSCOMB, NAS/NAE/NAM,[3] University of California, San Diego
MARTIN E. GLICKSMAN, NAE, Florida Institute of Technology
JENNIE S. HWANG, NAE, H-Technologies Group
CHRISTOPHER W. MACOSKO, NAE, University of Minnesota
C. KUMAR PATEL, NAS/NAE, Pranalytica, Inc.
BHAKTA B. RATH, NAE, Naval Research Laboratory
ALICE WHITE, Boston University

***Staff***

AZEB GETACHEW, Senior Program Assistant
LIZA HAMILTON, Associate Program Officer
EVA LABRE, Administrative Coordinator
JAMES P. MCGEE, Director
MARTIN OFFUTT, Senior Program Officer

[3] Member, National Academy of Medicine.

## LABORATORY ASSESSMENTS BOARD

ROSS B. COROTIS, NAE, University of Colorado, Boulder, *Chair*
WESLEY L. HARRIS, NAE, Massachusetts Institute of Technology
JENNIE S. HWANG, NAE, H-Technologies Group
ROBERT S. LANGER, NAS/NAE/NAM, Massachusetts Institute of Technology
W. CARL LINEBERGER, NAS, University of Colorado, Boulder
C. KUMAR N. PATEL, NAS/NAE, Pranalytica, Inc.
ELSA REICHMANIS, NAE, Georgia Institute of Technology
LYLE H. SCHWARTZ, NAE, U.S. Air Force Office of Scientific Research (retired)

***Staff***

AZEB GETACHEW, Senior Program Assistant
LIZA HAMILTON, Associate Program Officer
EVA LABRE, Administrative Coordinator
JAMES P. McGEE, Director
ARUL MOZHI, Senior Program Officer
MARTIN OFFUTT, Senior Program Officer

# Acknowledgment of Reviewers

This Consensus Study Report was reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise. The purpose of this independent review is to provide candid and critical comments that will assist the National Academies of Sciences, Engineering, and Medicine in making each published report as sound as possible and to ensure that it meets the institutional standards for quality, 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 thank the following individuals for their review of this report:

Daniel E. Atkins III, NAE,[1] University of Michigan,
Kenneth Birman, Cornell University,
Stuart Feldman, Schmidt Futures,
Butler W. Lampson, NAS[2]/NAE, Microsoft Research,
Jennifer Rexford, NAE, Princeton University, and
Stephen A. Vavasis, University of Waterloo.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations of this report nor did they see the final draft before its release. The review of this report was overseen by Robert F. Sproull, NAE, University of Massachusetts, Amherst. He was responsible for making certain that an independent examination of this report was carried out in accordance with the standards of the National Academies and that all review comments were carefully considered. Responsibility for the final content rests entirely with the authoring committee and the National Academies.

[1] Member, National Academy of Engineering.
[2] Member, National Academy of Sciences.

# Contents

# Summary

In 2018, at the request of the Director of the National Institute of Standards and Technology (NIST), the National Academies of Sciences, Engineering, and Medicine formed the Panel on Review of the Information Technology Laboratory of the National Institute of Standards and Technology (the "panel") and established the following statement of task:

> The National Academies shall appoint a panel to assess independently the scientific and technical work performed by four of the divisions of the National Institute of Standards and Technology (NIST) Information Technology Laboratory. This panel will review technical reports and technical program descriptions prepared by NIST staff and will visit the facilities of the Information Technology Laboratory. The visit will include technical presentations by NIST staff, demonstrations of NIST projects, tours of NIST facilities, and discussions with NIST staff. The panel will deliberate findings in closed sessions of the panel meeting and will prepare a report summarizing its assessment findings.

NIST specified that the following four divisions of the Information Technology Laboratory (ITL) would be reviewed: the Applied and Computational Mathematics Division (ACMD), the Advanced Network Technologies Division (ANTD), the Computer Security Division (CSD), and the Applied Cybersecurity Division (ACD). The panel was not asked to review the three other divisions of the ITL: the Information Access Division (IAD), the Software and Systems Division (SSD), and the Statistical Engineering Division (SED).

The NIST Director requested that the panel focus its assessment on the following factors: the technical quality of the work; the scientific expertise of the staff; the adequacy of facilities, equipment, and human resources; and the effectiveness with which outputs of the work are disseminated.

All four of the divisions reviewed are located in Gaithersburg, Maryland, and nearby Rockville, Maryland (at the National Cybersecurity Center of Excellence [NCCoE]), and were visited by the panel on June 12-14, 2018.

The divisions described their purposes as follows: perform research in the mathematical sciences to nurture trust in NIST metrology and scientific computing (ACMD); establish the technical basis for trustworthy networking via standards, measurement science, test methods, reference implementations, and guidance (ANTD); cultivate information technology's roots of trust (CSD); and improve the management of cybersecurity and privacy risk (ACD).

## CROSSCUTTING FINDINGS

The four ITL divisions reviewed by the panel work in areas of major national importance and vital relevance to the security and stability of computing systems and networks. The activities of the four divisions provide good coverage of both technology and theoretical/mathematical infrastructure, and they complement one another well. The formation of the NCCoE, a federally funded research and development center (FFRDC), has added substantially to the vitality of ITL by strengthening and deepening its interactions with the broader cybersecurity communities in both the private and the public sectors.

Risk in the security of computing systems and networks is expected to worsen rather than improve in the foreseeable future. ITL needs to continue to invest and deepen its involvement in these areas. It is important for ITL to establish an increased level of preparedness for responding to emergencies and to develop the necessary infrastructure and processes.

ITL has a major role to play internationally and has the credibility to do so. Stronger emphasis on the international role of ITL as convener, facilitator, and promulgator of standards is essential. A more prominent and active international role will be of significant benefit to the country's industrial and business sectors.

The detailed chapters on the four ITL divisions that form the core of this report provide overviews and appraisals and point to specific opportunities and challenges in each area. Three topics were highlighted in the findings of more than one division: staffing and recruitment, technical planning, and conferences and publications.

## Staffing and Recruitment

The long-term vitality of ITL is closely intertwined with its ability to continuously renew and deepen its pool of talent. This requires a strategic approach and coordinated efforts across ITL subdivisions. Closer collaboration with the country's universities can be helpful in this regard. In most cases, staffing is currently adequate to perform the assigned work. There are current and projected exceptions.

The ACMD is experiencing staffing stresses that may have an impact on its ability to meet its goal of providing comprehensive mathematical expertise for NIST. There is more demand for such expertise than can be met by the current ACMD staffing, and there is also an anticipation of substantial turnover due to the potential retirement of a significant fraction of staff in the near future.

> **RECOMMENDATION: The ACMD should evaluate its organizational and recruiting practices in order to better meet the challenges it faces. Ideas that should be considered include the use of contractors to broaden the pool of potential participants in the ACMD mission; the use of sabbatical opportunities for career staff to broaden the range of skills in response to new areas for ACMD; and development of a more effective pipeline for graduate students into ACMD through, for example, a broad-based university affiliates program.** (Chapter 6)

There is need to increase the core full-time ANTD staff to address new areas of research such as the Internet of Things (IoT), machine learning, and 5G wireless, and to expand existing areas of activity, such as formal verification and model checking.

> **RECOMMENDATION: The ANTD should build up and grow expertise in new and emerging areas such as the Internet of Things, machine learning, and 5G wireless.** (Chapter 6)

CSD's Lightweight Cryptography project promises good potential application if it receives greater visibility and resources.

> **RECOMMENDATION: The CSD should consider adding staff to the Lightweight Cryptography project.** (Chapter 6)

Another project whose impact could be amplified by additional resourcing and community outreach is the CSD's Combinatorial Methods in Software Testing project. The project currently has only two staff members.

**RECOMMENDATION: The CSD should consider adding staff to the Combinatorial Methods in Software Testing project to accelerate adoption of the project's tools and techniques by the software development community.** (Chapter 6)

The CSD's Vulnerability Metrics project has a critical short-term need for supplemental staff to address the increased volume and backlog of submissions for Common Vulnerabilities and Exposures (CVE) scoring.

**RECOMMENDATION: The CSD should devote additional short-term resources to Common Vulnerabilities and Exposures scoring until the backlog can be remediated.** (Chapter 6)

In the projects that are strategic national cybersecurity resources, the CSD is performing functions of a national laboratory. However, the CSD does not have recruiting programs like the national laboratories for mid-career staff.

**RECOMMENDATION: The CSD should emphasize recruiting of mid-career staff.** (Chapter 6)

NIST is limited to hiring U.S. citizens as permanent staff, but it also maintains a foreign guest researcher program, the Professional Research Experience Program (PREP), which supports visiting scientists and students under NIST-sponsored J1 visas.

**RECOMMENDATION: The ITL should expedite and grow the Professional Research Experience Program to hire more international graduate students from among those already at U.S. universities (e.g., as interns or cooperative researchers).** (Chapter 6)

Recruiting, retention, and mentoring of women and minorities has been a major issue in science, engineering, technology, and mathematics programs in organizations generally. ITL managers have expressed agreement with the importance of recruiting and developing women and minorities.

**RECOMMENDATION: The ITL should assess the effectiveness of its efforts to improve recruiting, retention, and mentoring of women and minorities.** (Chapter 6)

## Technical Planning

The technical work at the ACMD is driven by collaborations between ACMD staff and scientists from other disciplines, largely from other units within NIST. This work is mostly chosen in a bottom-up fashion, with some informal guidance from the division leader, so that there is little overt strategic organization of the scientific work done.

**RECOMMENDATION: The ACMD should engage in a formal strategic planning exercise with the following goals:**

- **Identify current core competencies and match them to NIST needs;**
- **Identify gaps and new opportunities—mapping what its strategic goals are to resources (budget and staff)—in emerging areas such as artificial intelligence and machine learning; and**
- **Engage the next generation of ACMD leaders in developing this plan, so that what emerges can be enthusiastically executed by them.** (Chapter 6)

Several of the ANTD projects had timelines and roadmaps, both short and long term. At the same time, these plans differ in their formats, making them hard to contrast with one another and evaluate thoroughly. A standard format template completed for each project could provide answers to a set of questions such as the following:

- What is the problem statement? (What is this project attempting to do?)
- Who is the ultimate customer? (Who will benefit if this project is successful?)
- Why should NIST use its resources to do this work? Why ANTD? Are adequate resources available?
- How does the proposed work build upon what already exists today in the external community?
- How will the results from the proposed work impact the external community?
- What are the measurable milestones that define the path toward success and completion?
- What is the execution plan? What resources will be used? What collaborations with other ITL/NIST organizations are needed to reach each milestone? What collaborations with industry or academia are needed to reach each milestone?

### Conferences and Publications

All divisions reported that their staff members attend professional conferences and author peer-reviewed publications. Anecdotal, but not systematic, data on conference attendance and publications, including the number of attendees, presenters, authors, and collaborative studies and the quality of the conferences and journals, were not made available to the panel.

> **RECOMMENDATION: The ITL should perform a systematic assessment of the conferences at which its staff members have presented their research or otherwise attended. The ITL should consider whether attendance has been sufficiently frequent and whether the conferences are of sufficiently high quality, and it should maintain or increase, as appropriate, conference attendance. A similar assessment should be performed for publications in scholarly journals.** (Chapter 6)

## DIVISION-SPECIFIC FINDINGS

### Applied and Computational Mathematics Division

As a research organization, the ACMD is very successful, considering several factors: executing high-quality research in applied and computational mathematics; meeting the needs of collaborators in diverse scientific disciplines; fulfilling its part of the institutional missions of NIST in metrology; and disseminating its work to broader communities. Especially noteworthy is its strength in mathematical analysis, particularly when used in tandem with simulation, which provides a high degree of scientific insight and is a distinctive strength of the ACMD. The ACMD successfully performs high-impact work in the areas of mathematics of metrology, high-performance computing and visualization, and materials modeling and simulation.

Notable accomplishments include the use of computer simulation in the development of a standard reference mortar to replace expensive oils in concrete rheometers; the design of standard reference artifacts for calibrating magnetic resonance imagers (MRIs); the deployment of community software for computing the physical properties of complex microstructures in solids from image data in three dimensions; the development of an efficient method for generation of uniformly distributed random bitstrings from a quantum source, with applications in secure communications; and developing and maintaining the Digital Library of Mathematical Functions, a project to update the National Bureau of Standards' renowned *Handbook of Mathematical Functions*.

The complexity of simulations of physical systems is rapidly increasing, and the processor architecture of computers used in simulation and modeling is becoming vastly more complex. There is a serious risk that the existing approach in ACMD of having a small number of people, or even a single staff member, implement complete simulation capabilities starting from scratch will no longer be feasible.

**RECOMMENDATION: The ACMD should evaluate simulation software development practices in light of the disruptive changes in high-performance computing technology.** (Chapter 2)

With the exception of staffing needs, ACMD resources appear adequate. The ACMD has an excellent group of career staff that requires expansion. A key facilities issue for the ACMD is access to evolving computing resources, although its current approach to sharing computing resources within NIST and extramurally appears to provide currently adequate access to computing capabilities.

ACMD staff members effectively perform a diverse set of activities in support of disseminating the outputs of their work. They publish extensively in high-visibility refereed journals and conference proceedings; distribute software, including micromagnetic modeling, tools for combinatorial testing of software, and the Digital Library for Mathematical Functions; and participate in standards setting for metrology, contributing to the publication of those standards in NIST reports.

### Advanced Network Technologies Division

The ANTD has four major project areas: Network Resilience, Cloud Computing, Internet of Things, and Future Network Technologies. ANTD's projects include testing methodology of indoor localization and tracking systems, wireless networks, wireless networking specifically for smart manufacturing, network resilience, robust interdomain routing, high-assurance domains, measurement for complex systems, a distributed algorithm for suppressing epidemic spread in networks, the NIST cloud computing program, software-defined networks and virtual networks, and information-centric networking.

Network localization and navigation (NLN) is an area in which NIST can play an important role in creating databases and through roadmapping exercises. ANTD's work in indoor localization is commendable. The ANTD has created a methodology to allow apples-to-apples comparisons of different smartphone-based NLN applications.

The Wireless Networking for Smart Manufacturing project is examining reliable wireless networking for smart manufacturing and industrial IoT by investigating the radio frequency (RF) landscape, channel sounding and modeling, co-simulation, and scheduling. By identifying key technological components to form a framework and reference model, the ANTD could help industrial and academic developers to contribute technological innovations toward standards. This would help secure a leading role of the United States in smart manufacturing technologies.

In the Complex Systems project, the ANTD has undertaken an ambitious effort to understand some of the emergent behaviors that pervade across a swath of complex systems that include social media and networks.

The Software-Defined and Virtual Networks project provides an excellent example of a well-articulated and well-contextualized research vision. The uMon (User-defined traffic MONitoring) project adheres to ANTD's goal of being a technology facilitator by creating a first step toward standardization.

While the ANTD has been active in pursuing projects in the information-centric networking (ICN) area, the future importance of such architectures is not assured. ANTD's role could beneficially be aligned with examining the fundamental networking problems that ICN is attempting to solve. The ANTD could also examine the efficacy of ICN as compared with traditional approaches. The division needs to leverage current efforts to explore commercially promising technologies such as mobile edge computing.

The Smart Grid is a key component of the nation's energy strategic plan. NIST is one of the federal agencies with a statutory role in the Federal Smart Grid Task Force,[1] led by the U.S. Department of Energy (DOE). Within the Smart Grid concept/architecture, the grid-to-end user interface is critical, and this is being addressed by ANTD staff. A roadmap for what the ANTD intends to accomplish in its Smart Grid project would be very helpful for evaluating the potential impact of this project.

ANTD's future benchmarks and data sets in cloud computing and related emerging areas such as data analytics systems could facilitate developers' and startup companies' choosing from among numerous open-source systems and standards. NIST's ability to convene stakeholders and assess pros and cons of various options makes this is an opportunity for real impact on both industry and academia.

**RECOMMENDATION: The ITL should develop and publish benchmarks to be used for evaluating the performance of existing and proposed networks and network technologies in more areas and should develop simulators and make them available for researchers.** (Chapter 3)

An important focus of research at NIST is measurement science for real systems. Today's ecosystem of public clouds, Internet service providers (ISPs), and the Internet offer myriad opportunities for doing this.

**RECOMMENDATION: The ITL should work with Internet service providers, public clouds, and data centers to collect data sets needed for NIST researchers to perform evaluations of the performance of existing networking solutions. If possible, the ITL should make those data sets available to industry and academia.** (Chapter 3)

One of the ITL's areas of expertise is the study of what problems need to be solved, rather than taking what is currently deployed and assuming that this was the right or only possible choice.

**RECOMMENDATION: In its role as a technology facilitator, the ITL should study Internet problems and behaviors, outside the assumptions inherent in deployed standards.** (Chapter 3)

Several ANTD projects focus on standardization and creation of International Organization for Standardization (ISO)[2]/NIST/Internet Engineering Task Force (IETF)[3] standards. For example, the Cloud Computing initiative resulted in an ISO standard, and the Secure Border Gateway Protocol (BGPSec) resulted in an IETF standard. ANTD's cloud computing effort involves work on catalyzing standards for Service Level Agreements (SLAs) into clouds, including federated clouds. NIST's involvement in the development of the ISO 19086 standard, which has since been adopted by Microsoft, is a commendable first step toward expansion of the Cloud Computing project in the ANTD. ANTD staff members in the High Assurance Domains project are encouraging adoption of IETF standards within the government.

[1] Further information is available at Department of Energy, "Federal Smart Grid Task Force," https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/federal-smart-grid-task-force.

[2] Further information is available at the International Organization for Standardization website athttps://www.iso.org.

[3] Further information is available at the Internet Engineering Task Force website at https://www.ietf.org.

Other ANTD projects focus on the creation of data sets. For example, the Indoor Localization project resulted in the PerFloc data sets.

Networking and network-based technologies such as cloud computing and data analytics systems are a fast-growing market. As such, increased investment in the ANTD would bolster existing expertise and enable ANTD growth into new areas as the need and opportunity arise.

## Computer Security Division

CSD's technology focus areas are cryptography, risk management, identity and access management, testing and validation, software security, vulnerability metrics and configurations, and emerging technologies.

The quality of work in CSD is uniformly excellent. Two CSD projects in particular are strategic national cybersecurity resources. The Cryptography project creates standards that are implemented by virtually every significant commercial encryption in a laptop computer, cell phone, or automated teller machine, and NIST's cryptographic standards are widely adopted by industry groups. The National Vulnerability Database (NVD) and the associated Common Vulnerability Scoring System are widely used, not only in government but also by private-sector firms and vulnerability and risk assessment product vendors.

The Quantum-Resistant Cryptography (QRC) project is timely and important, and its importance is well understood not only in the cryptographic community but also among government and commercial customers of cryptography. But because no quantum computer capable of breaking deployed public-key cryptosystems is likely to exist for at least 20 years, the QRC's impact will be felt on the time scale of decades. The Combinatorial Methods in Software Testing project is mature and has generated numerous highly cited publications. The tools and techniques developed by the project promise substantial impact on real-world software testing efficiency and effectiveness.

Other CSD projects could benefit from a clearer statement of the requirements that are driving them. The Access Control project has reached maturity and has had substantial academic and commercial impact, but it may have reached the point of diminishing return as an ITL activity.

> **RECOMMENDATION: The Access Control project's resources should be directed toward more recently emergent risks in order to have higher impact.** (Chapter 4)

The CSD has hired and retained appropriately expert staff in all of its project areas, but some projects could benefit from additional staff. Some emerging research areas will need to be staffed, and there are some issues relating to career progression and recruiting that could represent risks to the availability of necessary expertise in the medium term.

CSD's Lightweight Cryptography project is much less well-known to its potential customers than its QRC Algorithms Standardization project and its NVD and associated Common Vulnerability Scoring System.

> **RECOMMENDATION: The CSD should take steps to publicize the Lightweight Cryptography program among potential users of the resulting algorithms—particularly Internet of Things vendors and customers.** (Chapter 4)

Some emerging areas of research are currently being handled by existing CSD staff but will require dedicated experts as the areas mature. Additional staff expertise will shortly be required in the areas of multiparty computation, artificial intelligence (AI) and machine learning, high-performance computing security, and IoT security. The Pathways program has proven to be effective for recruiting scientific experts who eventually join CSD's permanent staff.

CSD facilities and equipment are adequate, and the budget for CSD staff to attend conferences and host workshops is adequate.

The CSD disseminates its work via Federal Information Processing Standards (FIPS), guidance in the form of NIST Special Publications, tools and testing services, academic publications, workshops, and data references, including online products such as the National Vulnerability Database (NVD). The CSD has long been a prolific producer and effective disseminator of high-quality and frequently cited publications, broadly implemented standards, and influential guidance.

CSD's impact is strong. Its guidelines and standards are widely adopted. However, evidence for the impact of many projects is anecdotal rather than systematic. Some projects have effective systematic impact metrics. Impact metrics would be very helpful in quantifying the effectiveness of the standards, guidance, and tools developed by the CSD.

> **RECOMMENDATION: Recognizing that impact is sometimes difficult to measure without deep insight into stakeholder products and processes, the ITL should work toward the development of impact metrics for projects in the CSD where development of such metrics is feasible.** (Chapter 4)

While the CSD and the ACD have incorporated privacy recommendations into their respective Risk Management guidance documents, there are no metrics for privacy.

> **RECOMMENDATION: The CSD, in partnership with the ACD, should investigate and, if possible, develop and disseminate metrics for privacy.** (Chapter 4)

### Applied Cybersecurity Division

The ACD addresses its goal of improving the management of cybersecurity and privacy risk through outreach and application of standards and best practices whose adoption is deemed necessary to strengthen U.S. cybersecurity capabilities. Central to its approach is collaboration with industry, other federal agencies, state and local agencies, academia, international organizations, and others. The division consists of three groups: the National Initiative for Cybersecurity Education (NICE); the Cybersecurity and Privacy Applications Group; and the NCCoE.

The NCCoE was established in 2012 by NIST in partnership with the state of Maryland and Montgomery County, Maryland. The NCCoE is an FFRDC operated by the MITRE Corporation. It houses about 30 laboratories, where researchers define cybersecurity issues, develop technical descriptions of problems, and engage with technology vendors that have standards-based, commercially available products that can be used as part of an example implementation.

NCCoE's Secure Interdomain Routing project is an effort to build a standards-based solution to a significant problem: spoofing routing information to hijack (reroute) packets on the Internet. The team has developed what appears to be a potentially cost-effective and thus practical solution for deployment, although a formal cost-benefit analysis has not yet been done.

The NCCoE initiated the Securing Wireless Infusion Pump project with the goal of applying the cybersecurity framework to devise a set of specific security measures that could enable health-care delivery organizations such as hospitals to use wireless infusion pumps for drug delivery without introducing undue risks. The project has delivered a valuable resource for direct application by hospitals and other health-care organizations. The publication *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*[4] does provide some general recommendations for mitigating and responding to residual risks. However, there is no indication in the document that those recommendations resulted from

[4] MITRE Corporation and NIST, 2017, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, Special Publication 1800-8, https://nccoe.nist.gov/projects/use-cases/medical-devices.

an adversarial analysis of the proposed solution. The infusion pump publication and other similar guidance documents produced by the NCCoE would benefit from such a review and also from a description of how these measures could be generalized to other venues.

It would be prudent for the ACD to consider how it would respond to a defeat scenario (a real-world safety or security problem after a technology has adhered to the best practices), technically and with communications to stakeholders, and to have a plan and assigned responsibilities ready in advance. Mature cybersecurity organizations create such response plans as a matter of course and find that they can mitigate many of the substantive and reputational consequences of dealing with such contingencies if they act quickly and consistently.

> **RECOMMENDATION: The ITL should consider putting together a rapid response plan of action to be invoked in the event of a real-world safety or security problem after a technology has adhered to the best practices and guidance from the NCCoE. To the extent that there is the potential for reputational damage to NIST as to the effectiveness of its best practices and guidance, the ACD should prepare in advance to proactively address issues that may arise.** (Chapter 5)

> **RECOMMENDATION: The NCCoE should add an adversarial perspective to the solutions and guidance that are promulgated by the NCCoE laboratories. That would mean conducting an adversarial review (e.g., red-teaming) against these solutions and feeding the adversarial review results back into their process for purposes of defensive improvement. This may involve adding steps into the current NCCoE process before reference designs and documents are released from the laboratory; additional resources should be added if needed to accomplish including the additional steps.** (Chapter 5)

> **RECOMMENDATION: The NCCoE should examine the university affiliates program with the federally funded research and development center contractor and consider how that program could be modified to enhance engagement with the existing university affiliates and how it could be improved to broaden participation with additional universities.** (Chapter 5)

The creation, enhancement, and sustainment of the NIST Cybersecurity Framework is one of the key contributions of the ACD and of the NIST cybersecurity program. The ACD recently updated the framework in response to Executive Order 13800,[5] and NIST has supported the framework by creating samples of framework profiles. The profiles are a critical resource for organizations that seek to adopt the framework. ACD is showing excellent commitment to sustaining the framework and enabling its adoption.

The National Initiative for Cybersecurity Education (NICE) framework provides classification of practitioner duties in both broad categories and specific professional roles. It has been generally accepted within the field and is being used to map certifications' common bodies of knowledge. The NICE group is also seeking to encourage collaboration and development of enhanced educational and training materials. The NICE initiative is of high quality and high impact. This effort is being recognized nationally and internationally for filling a significant need and doing so in a detailed fashion. There is strong interaction with multiple communities—education, government, and private sector—and the work appears to be well accepted.

The ACD Privacy Engineering Program helps technology managers navigate privacy engineering concerns via guidance such as NISTIR 8062, integrates the new privacy sensibilities into existing NIST Special Publications, and participates in collaborations, workshops, and standards bodies. ACD has

[5] The White House, 2017, "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11.

assembled talented staff with diverse perspectives that are carrying out this function with clarity and efficiency.

The NIST Identity and Access Management project has released a new family of guidelines (NIST Special Publications 800-63-3 and 800-63A-C) that focus on digital identity. This family of guidelines represents a significant evolution from the earlier versions of SP 800-63.

The ACD has built a first-rate team that focuses on the Cybersecurity Framework. The team combines a high level of cybersecurity expertise with an outstanding approach to stakeholder engagement and collaboration. The wide acceptance of the framework is ample testimony to their accomplishments in both technical cybersecurity and community engagement. Similarly, the NICE effort appears to be properly scoped and staffed. As the field continues to evolve, the NICE framework will need to continue to evolve as well, but the current personnel seem well positioned to track and incorporate changes as they occur.

In general, the scientific and technical talent was adequate for the projects and tasks that were undertaken by the ACD. Additionally, the research staff represented a diverse and inclusive mix of backgrounds, talent, and skills. For the research and testing conducted in the NCCoE laboratories, future research would benefit from having people with more adversarial experience in their backgrounds.

The ACD disseminates its outputs and interacts with extramural researchers and developers very well. Recognition of the Cybersecurity Framework is both industry-wide and worldwide and represents an example of a NIST project that is extremely well disseminated and recognized. Considerable effort is being devoted by the NICE project, with great effect, to dissemination of results and interaction with the community. The recently initiated Cybersecurity for the Internet of Things group appears to be connected with appropriate external organizations and is already in the process of developing a first document.

If problems arise in NCCoE products, NIST will need to be prepared to create updates and make users of the document aware that they have been released. The ACD, and in particular the NCCoE, would enhance its fulfillment of its practical, applied mission of strengthening the nation’s cybersecurity posture by proactively tracking and monitoring problems, attacks, and failures after solutions from the laboratories have been fielded.

> **RECOMMENDATION: The NCCoE should develop a process by which results from the field are systematically and proactively tracked and monitored after a project has been successfully transferred out of the NCCoE laboratory. The results from this proactive monitoring should then be disseminated (e.g., by the NIST Special Publications 1800 series) and appropriately incorporated into future NCCoE laboratory projects.** (Chapter 5)

# 1

# Introduction

The National Academies of Sciences, Engineering, and Medicine[1] has, starting in 1959, annually assembled panels of experts—from academia, industry, medicine, and other scientific and engineering communities of practice—to assess the quality and effectiveness of the National Institute of Standards and Technology (NIST) measurements and standards laboratories, of which there are now seven,[2] as well as the adequacy of the laboratories' resources. These reviews are conducted under contract at the request of the NIST.

In 2018, at the request of the NIST Director, the National Academies formed the Panel on Review of the Information Technology Laboratory of the National Institute of Standards and Technology (the "panel") and established the following statement of work:

> The National Academies shall appoint a panel to assess independently the scientific and technical work performed by the National Institute of Standards and Technology (NIST) Information Technology Laboratory. This panel will review technical reports and technical program descriptions prepared by NIST staff and will visit the facilities of the Information Technology Laboratory. The visit will include technical presentations by NIST staff, demonstrations of NIST projects, tours of NIST facilities, and discussions with NIST staff. The panel will deliberate findings in closed sessions of the panel meeting and will prepare a report summarizing its assessment findings.

NIST specified that the following four divisions of the Information Technology Laboratory (ITL) would be reviewed: the Applied and Computational Mathematics Division (ACMD); the Advanced Network Technologies Division (ANTD); the Computer Security Division (CSD); and the Applied Cybersecurity Division (ACD). All four of these divisions are located in Gaithersburg, Maryland, or nearby Rockville, Maryland (at the National Cybersecurity Center of Excellence [NCCoE]), and were visited by the panel on June 12-14, 2018.

The divisions described their purposes as follows: perform research in the mathematical sciences to nurture trust in NIST metrology and scientific computing (ACMD);[3] establish the technical basis for trustworthy networking via standards, measurement science, test methods, reference implementations, and guidance (ANTD);[4] cultivate information technology's roots of trust (CSD);[5] and improve the management of cybersecurity and privacy risk (AMD).[6]

[1] Effective July 1, 2015, the institution is called the National Academies of Sciences, Engineering, and Medicine (NASEM). References in this report to the National Research Council (NRC) are used in a historical context to refer to activities before July 1.

[2] The seven National Institute of Standards and Technology (NIST) laboratories are the Engineering Laboratory, the Physical Measurement Laboratory, the Information Technology Laboratory, the Material Measurement Laboratory, the Communication Technology Laboratory, the Center for Nanoscale Science and Technology, and the NIST Center for Neutron Research.

[3] NIST website, https://www.nist.gov/itl/math, accessed October 15, 2018.

[4] Abdella Batou, NIST, "Advanced Network Technologies Division," presentation to the panel, June 12, 2018.

[5] Matthew Scholl, NIST, "Computer Security Division," presentation to the panel, June 12, 2018.

[6] Kevin Stine, NIST, "Applied Cybersecurity Division," presentation to the panel, June 12, 2018.

TABLE 1.1 Personnel Working at the Information Technology Laboratory (ITL)

| Category | ITL (Total) | ACMD | ANTD | CSD | ACD |
|---|---|---|---|---|---|
| Full- and part-time or term | 344 | 42 | 18 | 86 | 39 |
| NIST fellows | 5 | 2 | 0 | 1 | 0 |
| Faculty | 13 | 5 | 1 | 2 | 0 |
| Contractor | 65 | 1 | 7 | 34 | 0 |
| Student/pathways internship | 23 | 0 | 4 | 7 | 1 |
| Post-doctorates | 6 | 4 | 0 | 0 | 0 |
| Detail (in) | 6 | 0 | 0 | 1 | 1 |
| Science emeritus | 1 | 0 | 0 | 0 | 0 |
| Guest researcher | 232 | 15 | 20 | 19 | 124 |
| Off-site collaborator | 30 | 4 | 0 | 0 | 22 |
| Volunteer | 1 | 0 | 0 | 0 | 0 |
| Student volunteer program | 4 | 2 | 0 | 0 | 1 |
| Student/high school intern Program | 0 | 0 | 1 | 0 | 0 |
| Student/summer undergraduate research fellow | 30 | 9 | 2 | 6 | 1 |
| TOTAL | 760 | 83 | 52 | 156 | 189 |

NOTE: The column ITL (Total) includes all divisions, not only the four under review. NOTE: ACMD = Applied and Computational Mathematics Division, ANTD = Advanced Network Technology Division, CSD = Computer Security Division, ACD = Applied Cybersecurity Division.

As of May 2018, there were 760 personnel working in ITL, roughly three-fifths of them in the four divisions reviewed, as shown in Table 1.1.

In 2015, a National Academies panel reviewed the other three divisions of the ITL—the Information Access Division, the Software and Systems Division, and the Statistical Engineering Division—and summarized its findings in a 2015 report.[7] In 2011, a National Academies panel reviewed all seven of the divisions of the ITL and summarized its findings in a 2011 report.[8]

For the current review, the NIST Director requested that the panel consider the following factors: the quality of the research and its relevance to the purposes of the divisions; the adequacy of the scientific expertise within the divisions; the adequacy of the divisions' facilities, equipment, and human resources; and the effectiveness by which the organization disseminates its program outputs.

The panel's approach to the assessment relied on the experience, technical knowledge, and expertise of its members. The panel reviewed selected examples of the technical research performed at the four divisions of ITL; because of time constraints, it was not possible to review the programs and projects of these four divisions exhaustively. The examples reviewed by the panel were selected by the ITL. The panel's goal was to identify and report salient examples of accomplishments, challenges, and opportunities for improvement with respect to the factors suggested above by the NIST Director. These examples are intended collectively to portray an overall impression of the laboratory, while preserving useful suggestions specific to the projects and programs that the panel examined. Given the necessarily broad and nonexhaustive nature of the review, omission in this report of any particular ITL program or project should not be interpreted as implying any negative reflection on the omitted program or project.

[7] NASEM, 2015, *Review of Three Divisions of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2015*, The National Academies Press. Washington, D.C.

[8] NRC, 2011, *An Assessment of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2011*, The National Academies Press, Washington, D.C.

# 2

# Applied and Computational Mathematics Division

## INTRODUCTION

The Applied and Computational Mathematics Division (ACMD) of the Information Technology Laboratory (ITL) "provides leadership within NIST in the use of applied and computational mathematics to solve science and engineering problems arising in measurement science and related applications."[1] The staff accomplishes this through research on analytical and numerical methods; high-performance computing and visualization; peer-to-peer collaborations to apply these to NIST problems; providing stewardship of mathematical reference data; and developing standards and tests for scientific computation. The division is organized into four groups of about equal size: Mathematical Analysis and Modeling, Mathematical Software, Computing and Communication Theory, and High-Performance Computing and Visualization.

## QUALITY OF THE RESEARCH

The technical projects in mathematics of metrology, high-performance computing and visualization, and materials modeling and simulation involve modeling in the applied physical sciences. This requires a combination of mathematical analysis and simulation. These involve collaborations between the ACMD and other laboratories within NIST, as well as collaborations with universities and other government agencies, including funding from the latter. These are areas in which the ACMD is strong and successful in performing high-impact work. Highlights include the use of computer simulation in the development of a standard reference mortar to replace expensive oils in concrete rheometers, the design of standard reference artifacts for calibrating magnetic resonance imagers (MRIs), and the deployment of community software for computing the physical properties of complex microstructures in solids from image data in three dimensions. A distinctive feature of ACMD's work in these areas is the integration of analytical methods with simulation to solve problems, as opposed to the use of simulation alone. This combined approach is a key feature of ACMD's success.

The work in quantum information science is focused on the investigation of fundamental mathematical questions in quantum computing and communications related to areas such as communications, cryptography, cybersecurity, randomness, clocks, and sensors. Some of this work is conducted through the NIST/University of Maryland Joint Center for Quantum Information and Computer Science, which is a multidisciplinary collaboration involving computer scientists and physicists at both institutions. A notable accomplishment in this area was development of an efficient method for generation of uniformly distributed random bitstrings from a quantum source, with applications in secure communications.

[1] National Institute of Standards and Technology (NIST), 2017, *Applied and Computational Mathematics Division: Summary of Activities for Fiscal Year 2017*, NISTIR 8208, NIST, Gaithersburg, Md., p. 3.

The work in foundations of measurement science for information systems includes a variety of topics in computer science and discrete mathematics. The topics include graph analysis, combinatorics, network security and reliability, and software testing, as well as interdisciplinary work in the Internet of Things (IoT).

The mathematical knowledge management area includes the Digital Library of Mathematical Functions, a highly successful project to update the National Bureau of Standards' *Handbook of Mathematical Functions*. The digital library uses Internet and graphical technologies to facilitate access to the information. This has led to the development of a widely used new version of the handbook as well as a heavily used website providing novel three-dimensional (3D) interactive graphical and visualization methods for displaying the properties of these functions. The website also provides links to software for evaluating special functions.

The complexity of simulations of physical systems is rapidly increasing. There is a need for higher model fidelity, such as replacing lower-dimensional models with fully 3D ones, representing more realistic complex geometries, and representing multiphysics and multiscale phenomena. In addition, the processor architecture of computers used in simulation and modeling is becoming vastly more complex, with deep memory hierarchies and heterogeneous compute engines with high degrees of parallelism on a single node. It is difficult to get even modest performance on such systems with existing programming tools, yet the need for higher fidelity representations will require it. There is a serious risk that the existing approach in the ACMD of having a small number of people, or even a single staff member, implement complete simulation capabilities starting from scratch will no longer be feasible.

**RECOMMENDATION: The ACMD should evaluate simulation software development practices in light of the disruptive changes in high-performance computing technology.**

## SCIENTIFIC EXPERTISE

The ACMD has an excellent group of career staff members. Their core expertise is in applied analysis and numerical methods that arise in the physical sciences, and mathematical techniques associated with theoretical computer science, particularly in problems related to quantum computing. A number of them have received professional recognition, including 2 NIST fellows (out of a total of 40 for all of NIST) and 8 fellows in various professional societies. The ACMD has a robust presence in leadership positions in the community, including membership on standards committees (6), journal editorial positions (14), and conference organizing committees (37). Another indicator of the technical strength of the organization is the large number of successful collaborations between ACMD staff and scientists from other disciplines that have led to many coauthored publications. The ACMD has also been successful in recruiting excellent postdoctoral researchers.

The demographics in the ACMD are shifting, and therefore anticipating multiple retirements is warranted. Losing talent will cause disruptions in various ACMD ongoing projects. However, adding professional staff could provide a clear opportunity to refresh, accelerate, or pivot in new directions or to add different ranges of expertise. The challenge of staff renewal is made more complicated by the inability to hire noncitizens as federal employees, thus reducing the pool of potential candidates for staff positions and for National Research Council (NRC) postdoctoral researchers. There are also far fewer graduate students involved in research activities than would be expected in an organization with the size and scientific visibility of the ACMD, a need that was specifically noted by ACMD staff.

## ADEQUACY OF FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

The ACMD is funded at a level of around $15.8 million per year (fiscal year 2018, estimated); one staff full-time equivalent (FTE) costs about $250,000 to $300,000 per year. Most of this is core funding (i.e., stable and noncompeted), with around $1.6 million per year awarded competitively either across the ITL or across NIST. This level of funding has been nearly flat over the last 5 years.

There are six technical project areas in ACMD: mathematics of metrology (to which 15 percent of the division's funds are allocated), high-performance computing and visualization (16 percent), materials modeling and simulation (16 percent), quantum information science (19 percent), foundations of measurement science for information systems (16 percent), and mathematical knowledge management (10 percent); the remaining 8 percent is division overhead funds or not yet allocated.

The computing landscape is changing radically due to disruptive changes in hardware and software, combined with the requirement for increasing fidelity of computer models. These changes have the potential of making infeasible the approach used in the ACMD of having small teams, or even single investigators, writing applications simulation codes from scratch.

The ACMD is experiencing large stresses that may have an impact on its ability to meet its goal of providing comprehensive mathematical expertise for NIST. There is more demand for such expertise than can be met by the current ACMD staffing, both in their core areas of expertise, and in new areas that require mathematical support, such as biomedical applications, machine learning, and the IoT. Simultaneously, there is an anticipation of substantial turnover due to the potential retirement of a significant fraction of staff in the near future, and difficulty recruiting new staff due to salary constraints and the requirement for U.S. citizenship. Responding to these stresses may require a more top-down level of strategic planning and deployment of resources than is currently employed by the ACMD.

One of the key facilities issues for the ACMD is access to evolving computing resources. Current requirements are met by a combination of compute servers and a visualization laboratory at the division level, NIST shared resources, and ad hoc access to external resources through the National Science Foundation (NSF) XSEDE and Department of Energy INCITE programs. This combination currently appears to provide adequate access to compute capabilities.

## DISSEMINATION OF OUTPUTS

The ACMD has a diverse set of activities in support of disseminating its work. ACMD staff members publish extensively in high-visibility refereed journals and conference proceedings. They also distribute software in a number of areas, including micromagnetic modeling, tools for combinatorial testing of software, and the aforementioned Digital Library for Mathematical Functions website and book. Through their participation in the standards setting for metrology, ACMD staff members contribute to the publication of those standards in NIST reports. They have also authored 46 journal publications and 34 conference publications, which have appeared in the last 18 months. More generally, their scientific enterprise is built on a culture of collaboration with other scientific disciplines, which leads to a broad dissemination of research ideas from the ACMD, resulting in high scientific impact.

As a research organization, the ACMD is very successful, considering several factors: executing high-quality research in applied and computational mathematics; meeting the needs of collaborators in diverse scientific disciplines; fulfilling the institutional missions of NIST in metrology; and disseminating its work to broader communities. Especially noteworthy is its strength in mathematical analysis, particularly when used in tandem with simulation, which provides a high degree of scientific insight and is a distinctive strength of the ACMD.

# 3

# Advanced Network Technologies Division

## INTRODUCTION

The Advanced Network Technologies Division (ANTD) of the Information Technology Laboratory (ITL) has four major project areas: Network Resilience, Cloud Computing, Internet of Things, and Future Network Technologies.

The ANTD's projects include testing methodology of indoor localization and tracking systems, wireless networks, wireless networking specifically for smart manufacturing, network resilience, robust interdomain routing, high-assurance domains, measurement for complex systems, a distributed algorithm for suppressing epidemic spread in networks, the NIST cloud computing program, software-defined networks and virtual networks, and information-centric networking.

## QUALITY OF THE RESEARCH

ANTD's portfolio of projects is varied. Some projects focus on standardization and creation of International Organization for Standardization (ISO)[1]/NIST/Internet Engineering Task Force (IETF)[2] standards. For example, the Cloud Computing initiative resulted in an ISO standard, and the Secure Border Gateway Protocol (BGPSec) resulted in an IETF standard. Some projects focus on the creation of data sets. For example, the Indoor Localization project resulted in the PerFloc data sets and competition.[3] Others focus on simulation (e.g., the Complex Systems and the Inter-Domain Routing projects). Several focus on basic innovative research. Commendably, many projects have external collaborators, including universities, other ITL divisions, the NIST Engineering Laboratory, and contractor companies.

### Indoor Localization Project

Network localization and navigation (NLN) is an area in which NIST can play an important role in creating databases and through roadmapping exercises. ANTD's work in indoor localization is commendable. The ANTD has created a methodology to allow apples-to-apples comparisons of different smartphone-based NLN applications. ANTD's database of measurements taken from representative buildings can be employed by ANTD personnel to evaluate the performance of proposed localization methodologies in future smartphones. This has enabled the testing of existing and new approaches to smartphone-based localization, demonstrating the important role of NIST in bringing together researchers

[1] Further information is available at the International Organization for Standardization website at https://www.iso.org.

[2] Further information is available at the Internet Engineering Task Force website at https://www.ietf.org.

[3] Further information is available at National Institute of Standard and Technology (NIST), "Rules of the PerfLoc Prize Competition," updated May 17, 2018, https://perfloc.nist.gov/perfloc-competition-rule.php.

and developers from industry—increasingly based in Asia—and academia, and in facilitating the progress in this field. The current database, supporting measurements (readily available to NLN applications) from the sensor outputs of existing smartphones, and actual building data (e.g., the actual location coordinates of wireless access points in each of several buildings) are being used to support the development of the ITL-standard NLN roadmap, which is in progress. This project will, presumably, be further extended to create a richer database that includes measurements from sensors, suitable for NLN, but not available on existing smartphones, and measurements (not readily available to NLN applications) from sensors that are on existing smartphones. The ANTD might consider making this database publicly accessible for direct use by non-ANTD researchers, product developers, and systems engineers in the evaluation of prospective NLN technologies and methodologies.

There is also a need for a network-level device-to-device channel simulator (accounting for spatiotemporal consistency as well as correlation among transmitters and receivers) that developers from industry and academia can use as a common basis for comparison. A good example is the QuaDRiGa channel simulator,[4] provided by the Fraunhofer Institute for Telecommunications, which offers a spatiotemporal consistency (at the transmitter side only). While this simulator is sufficient for cellular networks following the 3rd Generation Partnership Project (3GPP)[5] standardized channel models, it would require extensions for NLN to account for consistency at both the transmitter and receiver sides and for device-to-device links in NLN. Providing such capability for NLN (beyond cellular networks) would put NIST on the map as one of the key players in the field.

### Wireless Networking for Smart Manufacturing Project

Smart manufacturing is a growing and critical area of cyberphysical systems. Aligned with the mission of NIST, this project examines reliable wireless networking for smart manufacturing and the industrial Internet of Things (IoT) by investigating the radio frequency (RF) landscape, channel sounding and modeling, co-simulation, and scheduling. The project includes a plan to disseminate technology outcomes. Co-simulation and scheduling are heading in the right technological direction but need to focus more on flexible manufacturing scenarios referenced to industrial applications. Mechanisms such as consortia of industry and academia could be established as vehicles to support technological development and industrial deployment. The ANTD could proceed as a technology facilitator by utilizing the existing channel measurements and models, developed over the last several decades, and by identifying key technological components to form a framework and reference model, which would help industrial and academic developers to contribute technological innovations toward standards. This would help secure a leading role for the United States in smart manufacturing technologies.

### Robust Interdomain Routing Project

The ANTD has been involved in the development of the IETF BGPSec standards. Development of these standards is both important and challenging. Border Gateway Protocol (BGP) configuration is difficult and error-prone, and global repercussions have occurred. Secure BGP will address these problems, but it will also add complexity and performance overhead. This effort is not obviously aligned with NIST's unique niche in terms of framing problems and quantifying comparisons.

[4] Further information is available at the Quadriga website at http://quadriga-channel-model.de/#Start.

[5] Further information is available at the 3rd Generation Partnership Project website at https://www.3gpp.org.

## High-Assurance Domains Project

The IETF has defined several standards intended to solve problems such as SPAM and phishing. NIST is playing an important role by facilitating adoption of these standards. The ANTD is encouraging adoption of these standards within the government. This will help discover issues with these standards and will encourage the rest of the world to learn from NIST's experience. Project staff have published in a top conference, Usenix LISA. This gives them an opportunity to directly impact industry, gain visibility, and improve recruiting opportunities.

## Complex Systems Project

Complex systems are all around, and the ANTD has undertaken an ambitious effort to understand some of the emergent behaviors that pervade across a swath of complex systems that include social media and networks. The Network Resilience project, which includes the Complex Systems project, has collaborations with universities and a private company. There are two areas that the ANTD might revisit. First, simulation results need to be validated by real implementations in real systems. Concretely, several of the results on comparison of transmission control protocol (TCP) congestion control mechanisms, and their associated parameters, were done by simulation only, but they need to be strongly validated by actually implementing them in real networks like the Internet. Without this grounding, simulations are not convincing, regardless of the depth of the results from the simulator. (One organization that examines implementations in real networks is the Pantheon of Congestion Control.[6]) Second, ANTD presenters did not make clear the value of the external vendor who was being used to develop the simulator. Event-driven simulators (General Purpose Simulation System [GPSS]-based) are commonplace today, and existing open source simulators (e.g., ns-3[7]) may scale beyond the sizes in use by the vendor. It is critically important that the project look deeply into making a wise choice between using outsourced simulators and building in-house simulators. Building one's own simulator can give deep insight into the results, afford sufficient flexibility in repurposing the simulator for other aims, and afford NIST the opportunity to create an impact by standardizing its simulator for industrial and academic use. The choice needs to include consideration of whether the ITL can devote the appropriate level of resources.

## Epidemics Project

Epidemics in networks can disclose the fundamental behavior of complex communication networks. The Susceptible-Infected-Susceptible (SIS) model has been initially applied to develop a distributed algorithm suppressing epidemic spread in a connected network. Among widely scattered research outcomes in this multidisciplinary research, the ultimate goal and targeting applications of this project need to be identified by the ANTD in more realistic networking structures and operating network protocols. This is necessary so that appropriate models and sufficient scale can be defined to obtain more meaningful engineering outcomes. It would be useful to insert proper epidemic or automata models into scenarios involving patching of threats, which tend to be binary. Evaluations with more realistic networks—for example, small world and power law—and even real network traces—for example, from the Stanford Network Analysis Platform (SNAP) repository—are essential to convince researchers that the idea works in practice.

[6] Further information is available at the Stanford University Pantheon website at https://pantheon.stanford.edu/.

[7] ns-3 is a discrete-event network simulator. Further information is available at the NS-3 Consortium website at https://www.nsnam.org/.

### Cloud Computing Project

Given the growing level of extramural activity in cloud computing, an expanding ANTD effort could increase NIST's footprint and impact in the cloud computing area, including on the leading cloud providers. In particular, this effort needs to expand include development of benchmarks, data sets, and simulators for a broader focus area than Service Level Agreements (SLAs). The broadened focus area needs to include software offerings on public clouds (examples include Google BigQuery, AWS ElasticMapreduce, and Microsoft Azure; there are dozens of others); on new opportunistic modes of cloud computing (e.g., AWS Spot Instances and Google persistent instances); and on systems that run on these clouds (e.g., batch processing, real-time stream processing, and machine learning systems.). NIST is well positioned to do this work, and public clouds and data analytics systems are open resources with very little existing measurement and instrumentation studies. This is aligned with NIST's mission, and it presents an exciting opportunity for NIST impact on industry and academia.

### Software-Defined and Virtual Networks Project

The project on software-defined and virtual networks provides an excellent example of a well-articulated and well-contextualized research vision. The uMon project adheres to NIST's mission statement of being a technology facilitator by creating a first step toward standardization. The development of network measurement technologies within an open source software-defined networking environment seems to be a very appropriate research direction for NIST. The project progress thus far is encouraging, with good publications and strong partners in the effort. It will be important for the group to develop and follow a detailed roadmap as it continues to pursue this research. Any resulting network monitoring and measurement tools need to be made open access for possible wide adoption. The future plan of the project to engage with open consortia and move toward standardization of the uMon project is commendable.

### Information-Centric Networking Project

While the ANTD has been active in pursuing projects in the information-centric networking (ICN) area, the future importance of such architectures is not assured. ANTD's role could beneficially be aligned with examining the fundamental networking problems that ICN is attempting to solve. The ANTD could also examine the efficacy of ICN as compared with traditional approaches. ITL needs to leverage current efforts to explore commercially promising technologies such as mobile edge computing.

### Smart Grid Project

ANTD staff members have published two papers that reflect the division's activities relating to the Smart Grid, in *IEEE Transactions on Smart Grid* in 2015[8] and in *Proceedings of the IEEE* in 2017.[9]

[8] H. Gharavi and B. Hu, 2015, Scalable synchrophasors communication network design and implementation for real-time distributed generation grid, *IEEE Transactions on Smart Grid* 6(5):2539-2550.

[9] H. Gharavi and B. Hu, 2017, Synchrophasor sensor networks for grid communication and protection, *Proceedings of the IEEE* 105(7):1408-1428.

The Smart Grid has been recognized as a key component of the nation's energy strategic plan. NIST is one of the federal agencies with a statutory role in the Federal Smart Grid Task Force,[10] led by the U.S. Department of Energy (DOE) Within the Smart Grid concept/architecture, the grid-to-end user interface is critical, and this has been recognized by the ANTD staff. This interface must provide phase matching between the end user's electrical waveform and the main grid's electrical waveform at the point of interface. It must protect the main grid from various types of damage that could be induced by connecting end users. It must participate in the distributed management of reactive power flow. It must protect end users from damage induced by transients or faults on the main grid. It must enable secure two-way communication between entities connected to the grid. This interface must provide the necessary observability and controllability to quickly identify problems and to quickly isolate problems that occur at the points where the end users connect to the main network. At the same time, this interface must not provide a means for adversaries to simultaneously disable or destroy large portions of the grid and its connected entities. This is, appropriately, a key focus for the ANTD, the ITL, and NIST. NIST participation in (or leadership of) the creation of a set of technical requirements (and possibly uniform national standards) for this critical interface would be beneficial. Another aspect of the emerging Smart Grid where the ANTD is making contributions, and in which the ANTD needs to play a major role, is in the design of the communication networks that will be critical for the maintenance, protection, and control of the grid-to-end user interfaces, and all of the other entities that comprise the Smart Grid.

A roadmap for what ANTD intends to accomplish in its Smart Grid project would be very helpful for evaluating the potential impact of this project.

### Benchmarks, Simulator, and Data Sets

With respect to several of the research thrusts, including the Internet, clouds, IoT, wireless, and data analytics systems, the ANTD could have a much higher impact on industry and academia if it could provide new standardized benchmarks, simulators, and hosting/curation of data sets. In domains where developers have to choose among multiple systems or multiple protocols, it is useful to have standard benchmarks to help make this decision. In scenarios where new protocols were being developed (e.g., in IoT), standardized simulators can help validate the pros and cons of a protocol in a widely accepted way. Hosting of data sets is invaluable for validating new ideas, systems, and protocols using standard workload traces. Anonymization may be important; most current data sets are either maintained in academia or are occasionally released by companies. The PerFloc data set and competition, developed by the ANTD's Indoor Localization project, is exemplary, and other ANTD projects need to consider hosting data set.

Overall, the ANTD's future benchmarks and data sets in cloud computing and related emerging areas like data analytics systems could facilitate developers and startup companies choosing from among numerous open source systems and standards. NIST's ability to convene stakeholders and assess pros and cons of various options makes this is an opportunity for real impact on both industry and academia.

> **RECOMMENDATION: The ITL should develop and publish benchmarks to be used for evaluating the performance of existing and proposed networks and network technologies in more areas and should develop simulators and make them available for researchers.**

[10] Further information is available at Department of Energy, "Federal Smart Grid Task Force," https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid/federal-smart-grid-task-force.

### Study of Real Systems

An important focus of research at NIST is measurement science for real systems. Today's ecosystem of public clouds, Internet service providers (ISPs), and the Internet offer myriad opportunities for doing this. The ITL could profit from looking into studying data sets from ISPs, public clouds, and even private networks, perhaps improving instrumentation and measurement to facilitate data collection. In addition to using these for NIST research, the ANTD could help facilitate anonymization and other modifications to make these data sets into a form usable by industry and academia. NIST is positioned well to take advantage of its connections for this activity.

> **RECOMMENDATION: The ITL should work with Internet service providers, public clouds, and data centers to collect data sets needed for NIST researchers to perform evaluations of the performance of existing networking solutions. If possible, the ITL should make those data sets available to industry and academia.**

### Study of Internet Problems and Behaviors

One of ITL's areas of expertise is the study of what problems need to be solved, rather than taking what is currently deployed and assuming that this was the right or only possible choice. Interdomain routing is an important area that could benefit from the ANTD's expertise in framing problems. Although work on improving the specific protocol BGP is important, the ANTD need not assume that BGP was the only possible choice nor the right choice. An important area that has been largely ignored by the industry is studying what the "interdomain routing" problem is, outside the scope of a specific protocol. For instance, what policies are essential? Should some paths, even if physically there, be illegal or just discouraged? Should the source of the data be able to influence the path taken? What path-specific information might be secret?

> **RECOMMENDATION: In its role as a technology facilitator, the ITL should study Internet problems and behaviors, outside the assumptions inherent in deployed standards.**

## SCIENTIFIC EXPERTISE

The ANTD is in a high-impact area of research and development (R&D). The size of the ANTD staff has shrunk since 2011, when it had 29 full-time staff. This can be largely attributed to transfer of 13 staff members from the wireless group to the NIST Communication Technology Laboratory (CTL) in 2014. The ANTD appears to have tactically addressed this via an increase in guest researchers, from 2 guests in 2014 to 24 currently.

## ADEQUACY OF FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

The division has an overall budget of $5 million and an addendum budget that adds $3 million for specified projects.

Networking and network-based technologies such as cloud computing and data analytics systems are a fast-growing market. As such, increased investment in the ANTD would bolster existing expertise and enable ANTD growth into new areas as the need and opportunity arises.

Considering the demonstrated expertise of the existing staff, the existing roadmap, and the track record, to date, of enlisting the participation of academia and industry, the Indoor Localization project has sufficient resources to accomplish its proposed goals.

## DISSEMINATION OF OUTPUTS

Several ANTD projects focus on standardization and creation of ISO[11]/NIST/IETF[12] standards. For example, the Cloud Computing initiative resulted in an ISO standard, and the BGPSec resulted in an IETF standard. ANTD staff in the High-Assurance Domains project are encouraging adoption of IETF standards within the government. ANTD's cloud computing effort involves work on catalyzing standards for Service Level Agreements (SLAs) into clouds, including federated clouds. NIST's involvement in the development of the ISO 19086 standard, which has since been adopted by Microsoft, is a commendable first step toward expansion of the cloud computing project in ANTD.

Other ANTD projects focus on the creation of data sets. For example, the Indoor Localization project resulted in the PerFloc data sets and competition.

[11] Further information is available at the International Organization for Standardization website at https://www.iso.org.

[12] Further information is available at the Internet Engineering Task Force website at https://www.ietf.org.

# 4

# Computer Security Division

## INTRODUCTION

As documented in *Representative Examples of NIST Contributions to Cybersecurity*, [1] the NIST Computer Security Division (CSD) traces its history back to 1972. Its original projects, cryptography and risk management, are ongoing, alongside a variety of newer projects. Several years ago, the CSD's projects focused more on applications and some of the staff supporting those projects, together with the National Cybersecurity Center of Excellence (NCCoE), which was then part of the Information Technology Laboratory (ITL) Office, became the core for a new division: the Applied Cybersecurity Division (ACD), discussed in Chapter 5.

The division's technology focus areas are cryptography; risk management; identity and access management; testing and validation; software security, vulnerability metrics, and configurations; and emerging technologies. The CSD conducts joint work with the ACD and with other NIST ITL divisions—in particular, the Applied and Computational Mathematics Division (ACMD). CSD staff also collaborate extensively with academic researchers; more than 50 percent of CSD staff members who presented or published papers have external collaborators.

During the 2018 assessment, the CSD described the following projects: quantum-resistant cryptography, lightweight cryptography, FIPS 140 and the Crypto Module Validation Program (CMVP), derived credentials, access control, risk management, supply chain risk management, combinatorial methods in software testing, vulnerability metrics, and security for virtualized infrastructure.

CSD's fiscal year 2018 budget is $32.5 million, of which $17.8 million is designated for directed research projects. The CSD has supplemental funding of $4.5 million, of which $3.2 million is funding from other agencies and $1.3 million is income from testing and certification programs (e.g., the CMVP) and from the sale of test artifacts (e.g., test Personal Identification Verification [PIV] cards).

## QUALITY OF THE RESEARCH

The quality of work in CSD is uniformly excellent. Two CSD projects in particular are strategic national cybersecurity resources. The Cryptography project creates standards that are implemented by virtually every significant commercial encryption in a laptop computer, cell phone, or automated teller machine. NIST's cryptographic standards are widely adopted by industry groups. For example, the Payment Card Industry Security Standards Council requires FIPS 140-2 compliance as part of its Payment Card Industry Data Security Standards (PCI-DSS)[2] and Hardware Security Module (HSM) standards. Over the lifetime of the CMVP, the CSD has evaluated more than 24,000 cryptographic

[1] National Institute of Standards and Technology (NIST), 2018, *Representative Examples of NIST Contributions to Cybersecurity*, Gaithersburg, Md.

[2] Further information is available at the PCI Security Standards Council website at https://www.pcisecuritystandards.org/.

algorithm implementations, including 4,000 implementations of its symmetric-key Advanced Encryption Standard. CSD's latest cryptographic algorithm development effort, the Quantum-Resistant Cryptography (QRC) Algorithms Standardization project, received 69 submissions; 64 of these were found to meet the project's quality criteria, and they are in the process of being analyzed by NIST staff and the cryptographic community.

The National Vulnerability Database (NVD) and the associated Common Vulnerability Scoring System (CVSS) are widely used, not only in government but also by private-sector firms and vulnerability and risk assessment product vendors. As of June 2018, the NVD contained more than 103,000 distinct vulnerability entries. At the time of the discontinuation of MITRE's Common Vulnerabilities and Exposures (CVE) Compatibility Program in September 2017, 153 products and services from 84 organizations had been certified as CVE-compatible under the program.

Some CSD projects could benefit from more community outreach. The QRC project is timely and important, and its importance is well understood not only in the cryptographic community but also among government and commercial customers of cryptography. QRC's impact will be felt on the time scale of decades.

The Combinatorial Methods in Software Testing project is mature and has generated numerous highly cited publications. The tools and techniques developed by the project promise substantial impact on real-world software testing efficiency and effectiveness; even naïve applications of CST techniques can reduce the number of test cases required to reliably detect most faults by two orders of magnitude. The work on combinatorial methods in software testing could beneficially be broadly adopted across the software development world; it is a rare example of a technique that can improve both schedules and quality. Other CSD projects could benefit from a clearer statement of the requirements that are driving them.

The Access Control project has reached maturity and has had substantial academic and commercial impact, but it may have reached the point of diminishing return as an ITL activity. NIST's Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) standards have been broadly influential. RBAC is now a standard feature of most commercial security products' administrative subsystems. Commercial products from Oracle, SailPoint, and other vendors include robust RBAC features. ABAC is less broadly adopted by customers, but it is well supported by commercial security products for government use (e.g., from Jericho Systems), and for private-sector use (e.g., from Axiomatics and NextLabs). The 2011 National Research Council (NRC) panel report said this about the Access Control Project:

> As a general principle, given constraints on resources and the dynamic nature of IT security technology, the division should be mindful of the relevance of its research projects to the remainder of its mission and should be willing to sunset projects in those cases in which the project has begun to achieve industrial or commercial success or the focus of the project has diverged from the mainstream direction of information technology or from the division's work on standards and guidelines. The Role Based Access Control Program appears to have achieved a measure of industrial success and is perhaps a candidate for handing off to industry.[3]

The work of the Access Control Project is even more firmly established now in commercial practices and products than was the case in 2011.

**RECOMMENDATION: The Access Control project's resources should be directed toward more recently emergent risks in order to have higher impact.**

[3] National Research Council (NRC), 2011, *An Assessment of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2011*, The National Academies Press, Washington, D.C., p. 23.

## SCIENTIFIC EXPERTISE

The CSD has hired and retained appropriately expert staff in all of its project areas, but some projects could benefit from additional staff, some emerging research areas will need to be staffed, and there are some issues relating to career progression and recruiting that could represent risks to the availability of necessary expertise in the medium term.

CSD staff members exhibit a bimodal age distribution: there is a large pool of young expert staff members, fewer mid-career professionals, and a large population of late-career staff members. Twenty-seven percent of CSD staff members are currently retirement eligible; an additional 7 percent will be retirement eligible within 3 years. The concentration of retirement-eligible CSD staff represents a potential risk to the availability of expertise if government retirement programs or incentives change.

## ADEQUACY OF FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

The CSD's Lightweight Cryptography project is much less well-known to its potential customers than its QRC Algorithms Standardization project and its NVD and associated Common Vulnerability Scoring System. The Lightweight Cryptography project is not resourced as fully as the QRC project. The Lightweight Cryptography project currently has five staff members, all part time. Millions or even billions of Internet of Things (IoT) devices could be enabled for secure communications and data storage by the Lightweight Cryptography program in the near to medium term (the project aims to complete algorithm standardization in 2-4 years).

> **RECOMMENDATION: The CSD should take steps to publicize the Lightweight Cryptography program among potential users of the resulting algorithms—particularly Internet of Things vendors and customers.**

Supply chain risk management is a vast problem space, in which much research could be done. However, the CSD is having trouble finding and hiring staff qualified to work on supply chain risk analysis. It may be necessary to sharpen the focus of the Supply Chain Risk Analysis Project if additional staff cannot be added.

> **RECOMMENDATION: The ITL should consider conducting a threat and risk assessment to identify areas of greatest impact for future supply chain risk analysis work, the number and expertise of additional staff needed, and the appropriate focus of the work if additional staff cannot be hired.**

The Lightweight Cryptography and Combinatorial Methods in Software Testing projects both have the necessary core scientific expertise, but they could increase their impact if additional staff could be added. Also, expertise in supply chain security is limited in the market generally; hiring experts in this area, while desirable, may be difficult.

Some emerging areas of research are currently being handled by existing staff members but will require dedicated experts as the areas mature. Additional staff expertise will shortly be required in the areas of multiparty computation, artificial intelligence (AI) and machine learning, high-performance computing security, and IoT security. The Pathways program has proven to be effective for recruiting scientific experts who eventually join the CSD's permanent staff.

The CSD facilities and equipment are adequate, although more space would be welcome, particularly if additional staff members are added to the division. The budget for CSD staff to attend conferences and host workshops is adequate.

## DISSEMINATION OF OUTPUTS

The CSD disseminates its work via Federal Information Processing Standards (FIPS), guidance in the form of NIST Special Publications (SPs), tools and testing services, academic publications, workshops, and data references, including online products such as the National Vulnerability Database (NVD).

The CSD has long been a prolific producer and effective disseminator of high-quality, frequently cited publications, broadly implemented standards, and influential guidance. The 2011 NRC assessment cited above noted this history and cited examples; since that assessment NIST Cybersecurity staff have published 4 FIPS standards or standard updates, more than 150 Special Publications, more than 75 conference papers, and more than 65 journal papers. The CSD tracks these outputs carefully. The CSD's online resources, and especially the NVD, are also heavily utilized. However, these are production and dissemination metrics rather than impact metrics.

The CSD's impact is in fact strong; its guidelines and standards are widely adopted. However, evidence for the impact of many projects is anecdotal rather than systematic. Some projects have effective systematic impact metrics. The Cryptography project, for example, has a very useful impact metric; because the CSD is involved in the full life cycle of cryptographic technology development, from algorithm selection to standardization to validation. The CMVP serves as an impact metric collector by quantifying how many implementations of NIST algorithms are submitted for validation against the standards that the CSD publishes. The numbers are strong: the CMVP has validated more than 24,000 cryptographic module implementations over its lifetime, including 4,400 validations of implementations of CSD's Advanced Encryption Standard in products submitted by 497 companies. Across the CSD broadly, impact is less consistently measured than output and dissemination. Impact metrics could be quite valuable when making decisions about balancing CSD's relatively scarce resources across its projects.

Some important CSD projects, including Risk Management, Supply Chain Security, and Virtualization Security, perform well on production and dissemination metrics but have no systematic impact metrics. Impact metrics would be very helpful in quantifying the effectiveness of the standards, guidance, and tools developed by the CSD.

> **RECOMMENDATION: Recognizing that impact is sometimes difficult to measure without deep insight into stakeholder products and processes, the ITL should work toward the development of impact metrics for projects in the CSD where development of such metrics is feasible.**

One measure of project impact is the influence on international and commercial standards. The CSD cryptographic standards have had broad commercial and international adoption. Another recent example is the adoption of NIST SP-800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection* as the basis for the guidance in the draft ISO/IEC FDIS 21878 "Information Technology—Security Techniques—Security Guidelines for Design and Implementation of Virtualized Servers." The NIST Cybersecurity Framework, owned by the ACD, has also seen significant international adoption, which continues to grow—leading to a level of de facto international harmonization that is a major benefit for U.S. companies that operate worldwide.

One recommendation from the 2011 CSD assessment remains only partially addressed: "The CSD is also encouraged to investigate, as appropriate, NIST's role in metrics and guidelines for privacy, a subject that was not specifically presented to the panel."[4] While the CSD and the ACD have incorporated privacy recommendations into their respective Risk Management guidance documents, there are still no metrics. This subject has become more urgent since 2011.

[4] NRC, 2011, *An Assessment of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2011*, The National Academies Press, Washington, D.C., p. 23.

**RECOMMENDATION: The CSD, in partnership with the ACD, should investigate and, if possible, develop and disseminate metrics for privacy.**

On the topic of Risk Management guidance from the CSD and the ACD, the question of alignment between these bodies of work needs to be considered. The CSD has recently released an updated draft of SP 800-37 (revision 2)[5]—a core document in the SP800-39 series of Risk Management Framework (RMF) guidance. One of the stated objectives of this draft is to demonstrate how the Cybersecurity Framework can be aligned with the RMF and implemented using established NIST risk management processes. For its part, the ACD has recently published version 1.1 of the Cybersecurity Framework; that document states: "The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include NIST Special Publication (SP) 800-39.

The alignment of the NIST Risk Management Framework (owned by the CSD) and the NIST Cybersecurity Framework (owned by the ACD) is proceeding, but the work is not yet complete; the relevant documents are either in draft status or recently finalized. It is too early to tell how effective this alignment will be in organizations that implement both elements of NIST Risk Management guidance, and what adjustments to the guidance will be desirable.

**RECOMMENDATION: The CSD and the ACD should consider jointly hosting one or more implementer's workshops to test the emerging alignment of these two bodies of guidance.**

[5] NIST, 2018, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Draft NIST Special Publication 800-37: Revision 2, U.S. Department of Commerce, Washington, D.C.

# 5

# Applied Cybersecurity Division

## INTRODUCTION

The Applied Cybersecurity Division (ACD) of the Information Technology Laboratory (ITL) was spun out of the Computer Security Division (CSD) and established on October 1, 2015. Since the division is new, it has not previously been reviewed by a National Academies of Sciences, Engineering, and Medicine panel. The division addresses its goal of improving the management of cybersecurity and privacy risk through outreach and application of standards and best practices whose adoption is deemed necessary to strengthen U.S. cybersecurity capabilities. Central to its approach is collaboration with industry, other federal agencies, state and local agencies, academia, international organizations, and others. The division consists of three groups: the National Initiative for Cybersecurity Education (NICE); the Cybersecurity and Privacy Applications Group; and the National Cybersecurity Center of Excellence (NCCoE).

## QUALITY OF THE RESEARCH

### National Cybersecurity Center of Excellence

The NCCoE is central to the mission of the ACD. It was established in 2012 by NIST in partnership with the state of Maryland and Montgomery County, Maryland. The NCCoE exists as a federally funded research and development center (FFRDC) operated by the MITRE Corporation and is housed in a modern building about 60,000 square feet in size. Inside the building are about 30 laboratories, where researchers define cybersecurity issues, develop technical descriptions of problems, and engage with technology vendors that have standards-based, commercially available products that can be used as part of an example implementation. The NCCoE accesses expertise across universities through its Academic Affiliates Council.[1] Research is done to build a reference design, identify gaps in the build, and then continue to refine and harden the example implementation until there is a practical and usable reference design that addresses the cybersecurity challenge that inspired the project. The details of this completed reference design, standards mapping, laboratory implementation and more are issued in a three-volume NIST Special Publication (SP) 1800 series document.[2] Three projects that the NCCoE briefed to the panel were securing wireless infusion pumps, secure interdomain routing, and trusted cloud.

[1] In addition to the University of Maryland System, nine other universities from around the country are members: University of Alabama, Birmingham; University of Delaware; George Mason University; Massachusetts Institute of Technology; Purdue University; University of California, Berkeley; University of Illinois; University of Texas, Dallas; and University of Texas, San Antonio.

[2] The National Institute of Standards and Technology (NIST) Special Publication (SP) 1800 series documents “present practical, usable, cybersecurity solutions to the cybersecurity community. These solutions demonstrate how to apply standards-based approaches and best practices. An 1800 document can map capabilities to the

The NCCoE's Secure Interdomain Routing project is an effort to build a standards-based solution to a significant problem: spoofing routing information to hijack (reroute) packets on the Internet. The current routing system uses BGP (Border Gateway Protocol), and this is open to attacks by way of providing false information to sites performing routing.

The team involved, including contractor personnel, has built a working proof-of-concept model showing how to add protection to BGP. The solution uses a combination of roots of trusted information and PKI (Public Key Infrastructure) to authenticate routing changes. The solution appears to be compliant with the BGP standard and is thus plug-compatible with the current system. The solution appears to be potentially cost effective and thus practical for deployment, although a formal cost-benefit analysis has not yet been done.

This effort involved participation by many major Internet service provider (ISP) organizations, thus ensuring that the model developed will be compatible with existing practice and will help to accelerate any technology transfer to implementation.

The NCCoE-Secure Interdomain Routing group appears to have a workable, standards-compliant solution to the problem it is seeking to solve. The group needs to stress test and attack its solution to determine if it is, in fact, a complete solution. The group also has an opportunity to think a bit more broadly about its approach, and what else could be incorporated to enhance security—for example, including a notification step in its solution, such that sites that are targeted by spoofing attempts (directly or indirectly) can receive an alarm and trace information would provide for a stronger defense and initial forensics. BGP is a problematic protocol, however, so there are limits to what may be achievable.

In these very early days of cloud computing, one configures a machine model with desired hardware and software characteristics and assumes through contractual and reputational mechanisms that the machine will be provisioned as advertised. The NCCoE Trusted Cloud project explores how secure or measured boot technology employing a hardware root of trust can add engineering mechanisms into this mix to further ensure that one is not building on compromised foundations. Although the core technologies have been in existence for years, they are complicated and not widely used, and so they are at some risk of disappearing from future hardware designs. The ACD properly sees this as an excellent opportunity via the SP 1800 how-to guides to make hardened cloud computing more widely accessible.

Consistent with the NCCoE's goal to engage with vendor partners, the Trusted Cloud project included the involvement of Dell, IBM, Intel, Microsoft, RSA, VMware, and potentially other large cloud vendors not engaged during the early phase of NCCoE. It appears that the laboratory also possesses a network component that would allow the project to explore remote attestation.

Two directions for expanding the NCCoE-Trusted Cloud work could be (1) involving some security-sensitive cloud customers such as banks, to validate the benefits and hone the messaging; and (2) working with system administrators of operational large clouds to assess how the hardened individual machines can be managed at scale.

The NCCoE initiated the Securing Wireless Infusion Pump project with the goal of applying the cybersecurity framework to devise a set of specific security measures that could enable health-care delivery organizations such as hospitals to use wireless infusion pumps for drug delivery without introducing undue risks such as compromise of personal information or unauthorized modifications to drug dosage. Wireless infusion pumps are in wide use, and management of the risks they pose is important to public safety and security.

Five major vendors of wireless infusion pumps contributed resources and personnel to work with NIST and NCCoE staff to construct the guidelines. These vendors represent approximately 85 percent of the deployed equipment in the United States. In addition to their development of a standard that can be widely deployed, the companies were able to learn best practices that some are folding back into their product lines.

Cybersecurity Framework and outline steps needed for another entity or organization to recreate an example solution." See https://www.nist.gov/itl/nist-special-publication-1800-series-general-information, accessed August 28, 2018.

After reviewing the potential vulnerabilities of wireless infusion pumps, the project selected a security solution that is based on partitioning the hospital network to prevent malicious people or malware from gaining access to an infusion pump or pump server system. The project created a publication that provides detailed guidance on how to configure and lock down a network for organizations that wish to operate wireless infusion pumps securely. The project has delivered a valuable resource for direct application by hospitals and other health-care organizations.

While the infusion pump security solution has the potential to be a valuable resource for health-care delivery organizations, almost all security solutions can potentially be defeated by a sufficiently clever and determined adversary. Furthermore, complex solutions such as the network partitioning approach proposed for protecting infusion devices run a significant risk of being misconfigured by operators or users. The publication *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*[3] does provide some general recommendations for mitigating and responding to residual risks. However, there is no indication in the document that those recommendations resulted from an adversarial analysis of the proposed solution. The infusion pump publication and other similar guidance documents produced by the NCCoE would benefit from such a review.

Even with the best possible adversarial security review, there will remain some risk that a solution such as that in the infusion pump document could be defeated by a clever attacker. The consequences of such an event could be embarrassing or even hazardous. This is not a reason to avoid producing such solutions—to the contrary, well thought out solutions are of especially great value in such applications. However, it would be prudent for the ITL and the ACD to consider how they would respond to a defeat scenario, technically and with communications to stakeholders, and to have a plan and assigned responsibilities ready in advance. Mature cybersecurity organizations create such response plans as a matter of course and find that they can mitigate many of the substantive and reputational consequences of dealing with such contingencies if they act quickly and consistently.

**RECOMMENDATION: The ITL should consider putting together a rapid response plan of action to be invoked in the event of a real-world safety or security problem after a technology has adhered to the best practices and guidance from the NCCoE. To the extent that there is the potential for reputational damage to NIST as to the effectiveness of its best practices and guidance, the ACD should prepare in advance to proactively address issues that may arise.**

**RECOMMENDATION: The NCCoE should add an adversarial perspective to the solutions and guidance that are promulgated by the NCCoE laboratories. That would mean conducting an adversarial review (e.g., red-teaming) against these solutions and feeding the adversarial review results back into their process for purposes of defensive improvement. This may involve adding steps into the current NCCoE process before reference designs and documents are released from the laboratory; additional resources should be added if needed to accomplish including the additional steps.**

## CYBERSECURITY FRAMEWORK

The creation, enhancement, and sustainment of the NIST Cybersecurity Framework is one of the key contributions of the ACD and of the NIST cybersecurity program. The framework is mandatory for U.S. government agencies, and its adoption is proceeding across the federal government. Adoption by the private sector is voluntary, but critical infrastructure sectors—the financial sector is a key example—have chosen to adopt it, as have many individual organizations. The framework has also seen significant

[3] MITRE Corporation and NIST, 2017, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, Special Publication 1800-8, https://nccoe.nist.gov/projects/use-cases/medical-devices.

international adoption, which continues to grow, leading to a level of de facto international harmonization that is a major benefit for U.S. companies that operate worldwide.

The ACD recently updated the framework in response to Executive Order 13800,[4] and NIST has supported the framework by creating samples of framework profiles. The profiles are a critical resource for organizations that seek to adopt the framework. The ACD is showing excellent commitment to sustaining the framework and enabling its adoption.

While many people and organizations are aware of the NIST Cybersecurity Framework, the deep understanding necessary to adopt it effectively is uneven. The ACD's creation of sample profiles will assist organizations in the task of adoption and help to prevent cases where an organization deliberately or inadvertently claims to adopt the framework without taking appropriate action to determine and manage its cybersecurity risk. Creation of sample profiles is a key activity for the division and needs to be continued and emphasized. The NIST website that is the public face of the framework provides considerable useful information, but it is challenging for an organization that is new to the framework to find a concise answer to the question "I want to adopt the framework—what steps should I take and in what order?" NIST can provide organizations with an answer to this question with a modest investment of time and effort. Such an investment will pay major dividends for the nation and cybersecurity and needs to be undertaken. There may be some additional work required to advance the practical alignment between the Cybersecurity Framework version 1.1[5] and NIST Special Publication 800-37 on the Risk Management Framework (RMF).[6]

### National Initiative for Cybersecurity Education

The field of cybersecurity and privacy has undergone rapid expansion over the last two decades. Where once a single person could master a majority of the field, the knowledge and practices needed to work in the field have multiplied and diversified so that one person can no longer cover more than a fraction. To enable conversations about hiring, training, and education, a common framework of terms was needed. NIST provided this framework through the NICE and issued it as SP 800-181.[7]

The NICE framework provides classification of practitioner duties in both broad categories and specific professional roles. It has been generally accepted within the field and is being used to map certifications' common bodies of knowledge. It is also being used by professional organizations to map and describe elements of curricular recommendations. The recent Association for Computing Machinery (ACM)[8]/ Institute of Electrical and Electronics Engineers (IEEE)/International Federation for Information Processing (IFIP)[9] joint curricular recommendations are undergoing mapping to the guideline. In April, the Office of Personnel Management (OPM) issued guidance on use of the NICE framework to define federal jobs in the area of cybersecurity; some private sector entities are reportedly doing the same.

The NICE group is also seeking to encourage collaboration and development of enhanced educational and training materials. This effort is relatively recent but appears to be making good progress

[4] The White House, 2017, "Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

[5] NIST, 2018, *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1.*, Gaithersburg, Md.

[6] NIST, 2018, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Final Public Draft)*, Draft NIST Special Publication 800-37: Revision 2, Gaithersburg, Md.

[7] W. Newhouse, S. Keith, B. Scribner, and G. Witte, 2017, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST Special Publication 800-181, U.S. Department of Commerce, Washington, D.C.

[8] Further information is available at the Association of Computing Machinery website at https://www.acm.org.

[9] Further information is available at the International Federation for Information Processing website at https://www.ifip.org.

with its conferences, RAMPS project[10] to encourage new educational efforts, newsletters, and other activities.

The NICE group has also developed some resources, including a website, to help show hiring needs by practice area and national location (CyberSeek). This tool shows promise for guiding hiring and encouraging further training development.

The NICE initiative is of high quality and high impact. This effort is being recognized internationally as well as nationally for filling a significant need and doing so in a detailed fashion. There is strong interaction with multiple communities—education, government, and private sector—and the work appears to be well accepted. It is being integrated into those sectors to provide a common framework and definitions. The initial framework and the CyberSeek site are well done and highly useful for their intended audiences. The group is working on defining metrics and further guidance. These will be important for maintaining a leadership role in cyberspace education and training.

## Cybersecurity for the Internet of Things

As the cost of computing devices and communication continues to decrease, there is an acceleration of the movement to insert sensors and computational elements into a variety of elements in our environment—to connect "things" in a computational mass. This Internet of Things (IoT) presents new risks and challenges that are not being properly considered by all the developers and users of those "things."

This project within the ACD is focused on providing guidance to assess and mitigate risks in this evolving environment and to coordinate stakeholders, which is a challenge, since they are distributed globally. It is a nascent effort, but it builds on existing Information Technology Library projects and expertise. An initial report, NISTIR 8200, is under development.[11] The project is involved in several standards activities and working groups. Its goal is to better capture and define special needs and considerations of IoT systems. This effort will be informed by other ITL efforts, including the Cybersecurity Framework.

The Cybersecurity for the Internet of Things project is a new effort in a very important topic area. The effort is too new to draw any significant conclusions, other than to note that the personnel are pursuing appropriate initial goals. The market-definition of "things" is extraordinarily broad and growing. There is potential here for the group to be overwhelmed with the magnitude and scope of the problem set. It is important that strong leadership be exercised to keep the group focused on achievable important goals, and to keep alignment with other cybersecurity efforts within ITL, particularly within the NCCoE.

## Privacy Engineering

In recent years major Internet technology companies created a privacy engineering function that is distinct from security and legal concerns. Federal agencies holding data about individuals may be expected to staff that function as well. *Security* deals with risks from unauthorized access to data; *privacy* deals with risks from authorized access. Legal concerns include compliance obligations, met, for example, by clicking through terms of use and privacy policies. Engineering involves the construction of system features—for example, offering a map location timeline feature that provides an interesting activity memento but implicitly also illustrates what data are being collected. Privacy engineering is a new discipline that builds in predictability, manageability, and judicious protection of privacy, including

[10] Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) cybersecurity education and workforce development.

[11] NIST, 2018, *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, NISTIR 8200 (Draft), Gaithersburg, Md.

masking and anonymization. The ACD Privacy Engineering program helps technology managers navigate these choppy waters via guidance such as NISTIR 8062, integrates the new privacy sensibilities into existing NIST SPs, and participates in collaborations, workshops, and standards bodies. The ACD has assembled talented staff with diverse perspectives that are carrying out this function with clarity and efficiency.

### Identity and Access Management

The NIST Identity and Access Management project has released a new family of guidelines (NIST SPs 800-63-3[12] and 800-63A-C[13]) that focuses on digital identity. This family of guidelines represents a significant evolution from the earlier versions of SP 800-63. It takes a risk-based approach to identity standards and is compatible with modern technical approaches to identity and access management, such as new kinds of authentication tokens and pseudonymous identities. The new standard appears to be a significant improvement over its predecessors.

In addition to the content of the new standard, it is worth emphasizing the way that the ACD produced it. Two points are especially significant: (1) Rather than relying solely on drafts and calls for content, NIST also posted the drafts of the new documents on GitHub, a widely used open source software repository, and responded to comments on GitHub on a continuous basis. This process worked (the standards were produced), and it seems to have resulted in more public input, faster standard development, and a better and more widely accepted product. (2) The ACD integrated privacy engineering considerations into the development of the new standards. This is a proof point for the ACD's commitment to make privacy engineering a real and valuable technical discipline.

As future ACD programs undertake a similar approach to publication and public comment, the ACD may need to educate some new constituencies about the benefits of this approach and how to take advantage of it.

## SCIENTIFIC EXPERTISE

The ACD has built a first-rate team that focuses on the Cybersecurity Framework. The team combines a high level of cybersecurity expertise with an outstanding approach to stakeholder engagement and collaboration. The wide acceptance of the framework is ample testimony to their accomplishments in both technical cybersecurity and community engagement. Similarly, the NICE effort appears to be properly scoped and staffed. As the field continues to evolve, the NICE framework will need to continue to evolve as well, but the current personnel seem well-positioned to track and incorporate changes as they occur. The scope and nature of the Cybersecurity for the Internet of Things project is still being defined, but personnel appear to be appropriate and the team created for the new identity and access management initiative was very well suited to the task and brought significant expertise in the relevant technical and user interaction disciplines.

The NCCoE wireless infusion pump project was conducted by a team from NIST, the NCCoE FFRDC, and technical employees from infusion pump and security product developers who comprise a major fraction of the market for such products. Thus, the solution reflects significant expertise in security products and their use, and in the real-world configuration and operation of infusion pumps and related information technology (IT) systems. The expertise of this team is well suited to the project that it undertook. Similarly, the NCCoE Secure Interdomain Routing group has drawn on experienced personnel within ITL and the contractor operating the NCCoE FFRDC as well as a number of industry partners that

[12] NIST, 2017, *Digital Identity Guidelines,* NIST Special Publication 800-63-3, Gaithersburg, Md.

[13] NIST, 2017, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, NIST Special Publication 800-63A, Gaithersburg, Md.

operate significant portions of the Internet. This project helps to illustrate the potential of collaborative projects directed by NIST within the NCCoE, and the expertise of the team is also well suited to perform the currently assigned tasks.

The Cybersecurity Framework project needs to focus on the educational function of ensuring that potential adopters of the framework have clear and consumable information about what they should do to get started. This will be a small investment—perhaps requiring a new skillset—that will have a major payoff.

There did not appear to be evidence that the infusion pump project team included individuals with expertise in adversarial ("red-team") analysis of security solutions. The addition of such expertise to this and other similar NCCoE projects would provide a significant boost to product quality and credibility in the future.

In general, the scientific and technical talent was adequate for the projects and tasks that were undertaken. The research staff represented a diverse and inclusive mix of backgrounds, talent, and skills. For the research and testing conducted in the NCCoE laboratories, future research would benefit from having people with more adversarial experience in their backgrounds.

## ADEQUACY OF FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

The Cybersecurity Framework development effort is focused on identification and documentation of best practices and on community collaboration rather than experimentation or technical development. Based on its accomplishments, the project's resources appear to be sufficient for their task. In particular, the project appears to have sufficient resources for travel and for convening meetings and workshops—a critical aspect of their task. Similarly, the resources available to the NICE effort appear appropriate for the efforts at hand. The personnel are well qualified for the tasks being undertaken by the group. No specialized equipment or resources appear necessary at this time.

The resources for the Cybersecurity of the Internet of Things project appear to be appropriate. There will be strong interactions with other groups within the ACD as the project matures. There are several existing projects within the NCCoE that could be considered as part of the IoT domain, and those resources and their results may be useful to this group. Specialized resources may be necessary if specific types of "things" are evaluated—for example, security and privacy of fitness trackers, autonomous vehicles, and household appliances may require either obtaining a collection of such devices or collaborating with entities that have them.

The Identity and Access Management project appears appropriately resourced for the task it undertook. The team clearly learned from experience with the previous version of SP 800-63 and from the history of the National Strategy for Trusted Identities in Cyberspace (NSTIC) project. The significant resources allocated to the NSTIC program were reallocated to the NCCoE, with the effect that the ACD has fewer resources to commit to identity and access management than in the past. However, there was no sign that the team was inadequately resourced to meet its commitments.

The NCCoE wireless infusion pumps project benefited from the participation of equipment vendors who committed both equipment and people to the project. Commitment of this level of resources indicates a high level of industry enthusiasm for NCCoE and the infusion pump project. It is likely that this level of enthusiasm will result in broad operational adaptation and adoption of the solution that resulted from the project. Similarly, the NCCoE Secure Interdomain Routing project has an experimental testbed that appears to be adequate for model development. Access to systems provided by the industry partners needs to involve testing at scale and at Internet backbone speeds and volumes.

A project of the scope and credibility of the NCCoE wireless infusion pumps security effort is likely to attract broad interest in the medical device and cybersecurity communities. The latter attraction offers the ACD the opportunity to seek adversarial analysis and feedback that will make the solution more credible and effective. Such feedback can be solicited on a voluntary basis or by implementing a targeted "bug bounty" project to engage vulnerability researchers in security reviews. Such programs have been implemented widely in the IT industry and by some government agencies (e.g., Department of Defense).

While still relatively new, the NCCoE would benefit from greater breadth and depth in its engagement with university partners in the future. Improved university partner engagement will produce many benefits, including greater access to faculty and students who could potentially bring fresh new perspectives, approaches, and solutions to difficult technical challenges. Greater university engagement can assist in bringing additional adversarial perspectives into the NCCoE.

> **RECOMMENDATION: The NCCoE should examine the university affiliates program with the federally funded research and development center contractor and consider how that program could be modified to enhance engagement with the existing university affiliates and how it could be improved to broaden participation with additional universities.**

## DISSEMINATION OF OUTPUTS

Recognition of the Cybersecurity Framework is both industry-wide and worldwide and represents an example of a NIST project that is extremely well disseminated and recognized. While the Cybersecurity Framework is widely recognized and has already seen a high level of adoption, additional focus by the ACD on communicating the basics of the framework and how to adopt it will pay dividends in even broader adoption and even greater improvements in cybersecurity.

The NICE project is holding workshops and conferences on development of educational materials for the K-12 space, for post-secondary education, and for professional education. There is a newsletter published by the NICE office. NIST personnel from the group regularly attend and present at conferences and professional events, including, in recent months, the RSA conference and the Colloquium for Information Systems Security Education (CISSE) education conference. Considerable effort is being devoted, with great effect, to dissemination of results and interaction with the community beyond the publication of the Special Report.

The recently initiated Cybersecurity for the Internet of Things group appears to be connected with appropriate external organizations and is already in the process of developing a first document. The group has leadership with experience in dissemination of results from other projects.

The Privacy Engineering team is engaging with operators of federal information systems to prioritize privacy risks, offer solutions, and clear up confusion. Connected cars, smart cities, and ID systems are forward-looking examples. This commendable approach is a better fit for the privacy effort than laboratory experiments would be.

By using GitHub for dissemination and review of drafts, the Identity and Access Management project has introduced an innovative approach to the creation of NIST standards. The innovation extends to the publication of the identity and access management special publications as web pages rather than PDF documents. These changes will help the ACD to be seen as an organization that is operating in the world of the Internet.

Some individuals and organizations may be put off by innovations such as the use of GitHub for the dissemination of identity and access management project results. It may be appropriate for the ACD to watch for resistance or negative feedback and ensure that it is clear with stakeholders about what has and has not changed in the standards development process.

The product of the NCCoE wireless infusion pumps project is a well-structured document that includes clear explanatory text and sufficient technical detail for applying the solution. It is very usable, and the fact that many vendors participated in the creation of the solution makes it likely that the document will receive broad distribution to an interested audience. The infusion pump project is a good model for the creation of NCCoE products that are likely to be used.

The NCCoE Secure Interdomain Routing group has a plan for appropriate dissemination of the results, but the effort is not yet to a level of maturity where that is appropriate. The presence of industry partners in the project suggests a robust technology transfer path for the results. If problems arise in NCCoE products, NIST will need to be prepared to create updates and make users of the document aware that they have been released. Software development organizations, for example, create regular updates (patches) and publicize their release. Preparing a plan for updating guidance documents and publicizing the fact that an update has been released would be very worthwhile. Advance planning will make the process go smoother and mitigate negative consequences.

The ACD, and in particular the NCCoE, would enhance its fulfillment of its practical, applied purpose of strengthening the nation's cybersecurity posture, by proactively tracking and monitoring problems, attacks, and failures after solutions from the laboratories have been fielded. Problems will occur in the real world that were not anticipated in the laboratory. It is important that the systematic tracking of these results from the field be reported as part of the NCCoE dissemination process and fed forward into future laboratory projects.

**RECOMMENDATION: The NCCoE should develop a process by which results from the field are systematically and proactively tracked and monitored after a project has been successfully transferred out of the NCCoE laboratory. The results from this proactive monitoring should then be disseminated (e.g., by the NIST Special Publications 1800 series) and appropriately incorporated into future NCCoE laboratory projects.**

# 6

# Crosscutting Findings

This chapter summarizes findings that apply across multiple divisions NIST's Information Technology Laboratory (ITL). These findings are in the areas of staffing and recruitment, technical planning, and conferences and publications.

## STAFFING AND RECRUITMENT

In most cases staffing is currently adequate to perform the assigned work. There are current and projected exceptions.

The Applied and Computational Mathematics Division (ACMD) is experiencing staffing stresses that may have an impact on its ability to meet its goal of providing comprehensive mathematical expertise for NIST. There is more demand for such expertise than can be met by the current ACMD staffing, both in their core areas of expertise and in new areas that require mathematical support, such as biomedical applications, machine learning, and the Internet of Things (IoT). There is also an anticipation of substantial turnover due to the potential retirement of a significant fraction of staff in the near future. Recruiting new staff is difficult due to salary constraints and the requirement for U.S. citizenship. Responding to these stresses may require a more top-down level of strategic planning and deployment of resources than is currently employed by ACMD.

> **RECOMMENDATION: The ACMD should evaluate its organizational and recruiting practices in order to better meet the challenges it faces. Ideas that should be considered include the use of contractors to broaden the pool of potential participants in the ACMD mission; the use of sabbatical opportunities for career staff to broaden the range of skills in response to new areas for ACMD; and development of a more effective pipeline for graduate students into the ACMD through, for example, a broad-based university affiliates program.**

There is opportunity to increase the core full-time Advanced Network Technologies Division (ANTD) staff to address new areas of research such as IoT, machine learning, and 5G wireless and to expand existing areas of activity such as formal verification and model checking.

> **RECOMMENDATION: The ANTD should build up and grow expertise in new and emerging areas such as the Internet of Things, machine learning, and 5G wireless.**

The Computer Security Division (CSD)'s Lightweight Cryptography project promises good potential application if it receives greater visibility and resources.

**RECOMMENDATION: The CSD should consider adding staff to the Lightweight Cryptography project.**

Another project whose impact could be amplified by additional resourcing and community outreach is the Combinatorial Methods in Software Testing project. The project currently has only two staff members.

**RECOMMENDATION: The CSD should consider adding staff to the Combinatorial Methods in Software Testing project to accelerate adoption of the project's tools and techniques by the software development community.**

The Vulnerability Metrics project has a critical short-term need for supplemental staff. The project has among its responsibilities the scoring of Common Vulnerabilities and Exposures (CVE) submissions to the National Vulnerability Database (NVD). A recent change in the methodology for submission of CVEs has resulted in an increased volume of submissions, which has in turn resulted in a backlog of unscored CVEs at the CSD. The CSD is working on automation technology that should eliminate this problem in the medium term, but since the NVD is a strategic national cybersecurity resource, a short-term backlog has likely negative implications both for the state of U.S. cybersecurity and for NIST's reputation as a trusted provider of this information. Recent changes in CVE submission have resulted in a Common Vulnerability Scoring System (CVSS) backlog at CSD. The CVSS backlog is a reputation risk to NIST and a security risk to the community.

**RECOMMENDATION: The CSD should devote additional short-term resources to Common Vulnerabilities and Exposures scoring until the backlog can be remediated.**

The CSD is in essence performing the functions of a national laboratory, in its strategic national cybersecurity programs (the Cryptography program and the National Vulnerability Database). However, CSD does not have academic outreach and recruiting initiatives like those of the national laboratories, especially for mid-career staff, to attract researchers to these strategic programs. For strategic projects, the CSD may need to engage more deeply with mid-career Ph.D. professionals in order to recruit required technical talent going forward.

**RECOMMENDATION: The CSD should emphasize the recruiting of mid-career staff.**

Should the Cybersecurity Framework project move ahead with an effort to improve the understandability and consumability of the framework, the ACD may require additional staff or staff members with backgrounds in communicating technical results rather than development and documentation of cybersecurity practices.

NIST is limited to hiring U.S. citizens as permanent staff, but it also maintains a foreign guest researcher program that supports visiting scientists and students under NIST-sponsored J1 visas. Recently the Professional Research Experience Program (PREP)[1] has been proposed by NIST to provide another source of student appointment. Unfortunately, ANTD staff reported that the PREP has not yet been initiated.

NIST's PREP needs to be kicked off the ground urgently and grown in the coming years. This offers a prime opportunity to tap into the large pool of international graduate students who are already at

[1] "The new NIST-wide Professional Research Experience Program (PREP) is designed to provide valuable laboratory experience and financial assistance to undergraduate, graduate and post-graduate students." See https://www.nist.gov/iaao/academic-affairs-office/nist-professional-research-experience-program-prep, accessed August 20, 2018.

U.S. universities, as guest researchers but also as future full-time staff. The PREP also promises to offer increased interaction with universities.

**RECOMMENDATION: The ITL should expedite and grow the Professional Research Experience Program to hire more international graduate students from among those already at U.S. universities (e.g., as interns or cooperative researchers).**

Recruiting, retention, and mentoring of women and minorities has been a major issue in science, technology, engineering, and mathematics programs in organizations generally. Creation of a diversity plan that is clear and flexible, and a conscious set of steps to implement the plan, are needed.

ANTD managers expressed a desire to recruit more women and minorities; supporting data on demographics were not provided. While a plan for mentoring women and minority staff was mentioned, the panel did not interact with a sufficient number of women to form an impression of its status or impact. Some ANTD managers reported that there are women only among the guest researchers and very few (or none, in some divisions) among the permanent Information Technology Library staff. Recruiting women and minorities could be assisted by the development of a concrete plan for recruiting, retention, and mentoring of women and minority staff. Such a plan could be revised and revisited for improvement after each recruiting year.

**RECOMMENDATION: The ITL should assess the effectiveness of its efforts to improve recruiting, retention, and mentoring of women and minorities.**

## TECHNICAL PLANNING

The technical work at the ACMD is driven by collaborations between ACMD staff and scientists from other disciplines, largely from other units within NIST. These researchers are mostly chosen in a bottom-up fashion, with some informal guidance from the division leader, so that there is little overt strategic organization of the scientific work done. Many of the collaborations involve one or two members of the ACMD, often at a part-time level of effort. There is no comprehensive strategic plan to set priorities and allocate resources. The most recent comprehensive strategic planning exercise for the ACMD was performed a decade ago. This is particularly problematic in light of the fact that the demand for mathematical expertise in NIST far exceeds the resources available to the ACMD, both in the areas of traditional strength and in emerging areas such as machine learning and the IoT, which have been identified as important by ITL management.

**RECOMMENDATION: The ACMD should engage in a formal strategic planning exercise with the following goals:**

- **Identify current core competencies and match them to NIST needs;**
- **Identify gaps and new opportunities—mapping what their strategic goals are to resources (budget and staff)—in emerging areas such as artificial intelligence and machine learning; and**
- **Engage the next generation of ACMD leaders in developing this plan, so that what emerges can be enthusiastically executed by them.**

Several of the ANTD projects had timelines and roadmaps, both short and long term. At the same time, these plans differ in their formats, making them hard to contrast with one another and evaluate thoroughly. A standard format template completed for each project could provide answers to a set of questions describing aspects of the project. This will help articulate the project to others, but if not overly prescriptive, would leave room for creativity and pivoting during the execution of each project. The template could include questions such as the following:

- What is the problem statement? (What is this project attempting to do?)
- Who is the ultimate customer? (Who will benefit if this project is successful?)
- Why should NIST use its resources to do this work? Why ANTD? Are adequate resources available?
- How does the proposed work build upon what already exists today in the external community?
- How will the results from the proposed work impact the external community?
- What are the measurable milestones that define the path toward success and completion?
- What is the execution plan? What resources will be used? What collaborations with other ITL/NIST organizations are needed to reach each milestone? What collaborations with industry or academia are needed to reach each milestone?

## CONFERENCES AND PUBLICATIONS

All ITL divisions reported that their staff members attend professional conferences and author peer-reviewed publications. Conferences are among the best places to interact with the top graduate students from across the United States and the world. Aside from creating a direct impact on industry, presence and presentations at top conferences—some of which accept only a fraction of the submitted papers—create visibility to graduate students and communicate to these students that NIST is an exciting place to work. Anecdotal, but not systematic, data on conference attendance and publication, including the number of attendees, presenters, authors, and collaborative studies and the quality of the conferences and journals, were not made available to the panel.

**RECOMMENDATION: The ITL should perform a systematic assessment of the conferences at which its staff members have presented their research or otherwise attended. The ITL should consider whether attendance has been sufficiently frequent and whether the conferences are of sufficiently high quality, and it should maintain or increase, as appropriate, conference attendance. A similar assessment should be performed for publications in scholarly journals.**

# Acronyms

| | |
|---|---|
| 3D | three-dimensional |
| 3GPP | 3rd Generation Partnership Project |
| ABAC | Access-Based Access Control |
| ACD | Applied Cybersecurity Division |
| ACM | Association of Computing Machinery |
| ACMD | Applied and Computational Mathematics Division |
| AI | artificial intelligence |
| ANTD | Advanced Network Technologies Division |
| BGP | Border Gateway Protocol |
| BGPSec | Secure Border Gateway Protocol |
| CMVP | Crypto Module Validation Program |
| CSD | Computer Security Division |
| CTL | Communications Technology Laboratory |
| CVE | Common Vulnerabilities and Exposures |
| CVSS | Common Vulnerability Scoring System |
| DOE | Department of Energy |
| FFRDC | federally funded research and development center |
| FIPS | Federal Information Processing Standards |
| FTE | full-time equivalent |
| GPSS | General Purpose Simulation System |
| HSM | Hardware Security Model |
| IAD | Information Access Division |
| ICN | information-centric networking |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IFIP | International Federation of Information Processing |
| INCITE | Innovative and Novel Computational Impact on Theory and Experiment |
| IoT | Internet of Things |
| IoTDI | Internet of Things Design and Implementation |
| ISO | International Organization for Standardization |
| ISP | Internet service provider |
| ITL | Information Technology Laboratory |

| | |
|---|---|
| NCCoE | National Cybersecurity Center of Excellence |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| NLN | network localization and navigation |
| NRC | National Research Council |
| NSF | National Science Foundation |
| NSTIC | National Strategy for Trusted Identities in Cyberspace |
| NVD | National Vulnerability Database |
| OPM | Office of Personnel Management |
| PCI-DSS | Payment Card Industry Data Security Standard |
| PIV | Personal Identification Verification |
| PKI | Public Key Infrastructure |
| PREP | Professional Research Experience Program |
| QRC | Quantum-Resistant Cryptography |
| R&D | research and development |
| RBAC | Role-Based Access Control |
| RF | radio frequency |
| RMF | Risk Management Framework |
| SED | Statistical Engineering Division |
| SIS | Susceptible-Infected-Susceptible |
| SLA | Service Level Agreement |
| SNAP | Stanford Network Analysis Platform |
| SP | Special Publication |
| SSD | Software and Systems Division |
| TCP | transmission control protocol |