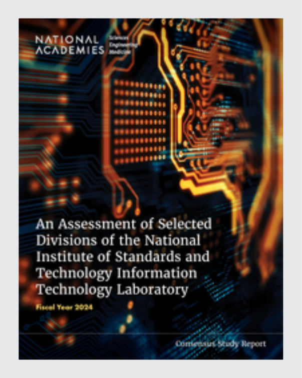
NATIONAL ACADEMIES Sciences Engineering Medicine

NATIONAL ACADEMIES PRESS
Washington, DC

This PDF is available at http://nap.nationalacademies.org/27430



# An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024 (2025)

## DETAILS

84 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-71407-5 | DOI 10.17226/27430

## CONTRIBUTORS

Panel on Assessment of the National Institute of Standards and Technology (NIST) Information Technology Laboratory; Laboratory Assessments Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

## SUGGESTED CITATION

National Academies of Sciences, Engineering, and Medicine. 2025. *An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024*. Washington, DC: The National Academies Press. https://doi.org/10.17226/27430.

BUY THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at nap.edu and login or register to get:

- Access to free PDF downloads of thousands of publications
- 10% off the price of print publications
- Email or social media notifications of new titles related to your interests
- Special offers and discounts

All downloadable National Academies titles are free to be used for personal and/or non-commercial academic use. Users may also freely post links to our titles on this website; non-commercial academic users are encouraged to link to the version on this website rather than distribute a downloaded PDF to ensure that all users are accessing the latest authoritative version of the work. All other uses require written permission. (Request Permission)

This PDF is protected by copyright and owned by the National Academy of Sciences; unless otherwise indicated, the National Academy of Sciences retains copyright to all materials in this PDF with all rights reserved.

NATIONAL ACADEMIES
*Sciences*
*Engineering*
*Medicine*

NATIONAL
ACADEMIES
PRESS
Washington, DC

# An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory

## Fiscal Year 2024

Panel on Assessment of the National Institute
of Standards and Technology (NIST)
Information Technology Laboratory

Laboratory Assessments Board

Division on Engineering and Physical Sciences

Consensus Study Report

Copyright National Academy of Sciences. All rights reserved.

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

This activity was supported by task order 1333ND24FNB100003 under contract 1333ND23DNB100003 between the National Academy of Sciences and 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: 978-0-309-71407-5
International Standard Book Number-10: 0-309-71407-9
Digital Object Identifier: https://doi.org/10.17226/27430

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.

Copyright 2025 by the National Academy of Sciences. National Academies of Sciences, Engineering, and Medicine and National Academies Press and the graphical logos for each are all trademarks of the National Academy of Sciences. All rights reserved.

Printed in the United States of America.

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2025. *An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024*. Washington, DC: The National Academies Press. https://doi.org/10.17226/27430.

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. John L. Anderson is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The National Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.nationalacademies.org**.

Copyright National Academy of Sciences. All rights reserved.

**Consensus Study Reports** published by the National Academies of Sciences, Engineering, and Medicine document the evidence-based consensus on the study's statement of task by an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and the committee's deliberations. Each report has been subjected to a rigorous and independent peer-review process and it represents the position of the National Academies on the statement of task.

**Proceedings** published by the National Academies of Sciences, Engineering, and Medicine chronicle the presentations and discussions at a workshop, symposium, or other event convened by the National Academies. The statements and opinions contained in proceedings are those of the participants and are not endorsed by other participants, the planning committee, or the National Academies.

**Rapid Expert Consultations** published by the National Academies of Sciences, Engineering, and Medicine are authored by subject-matter experts on narrowly focused topics that can be supported by a body of evidence. The discussions contained in rapid expert consultations are considered those of the authors and do not contain policy recommendations. Rapid expert consultations are reviewed by the institution before release.

For information about other products and activities of the National Academies, please visit www.nationalacademies.org/about/whatwedo.

Copyright National Academy of Sciences. All rights reserved.

## PANEL ON ASSESSMENT OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) INFORMATION TECHNOLOGY LABORATORY

**KWANG-CHENG CHEN**, University of South Florida, *Chair*
**GAIL-JOON AHN**, Arizona State University
**JANDRIA S. ALEXANDER**, Booz Allen Hamilton
**STEVEN M. BELLOVIN (NAE)**, Columbia University
**THOMAS A. BERSON (NAE)**, Anagram Laboratories
**CHARLES BLAUNER**, CyberAegis and Team8
**RUSSEL E. CAFLISCH (NAS)**, Courant Institute of Mathematical Sciences, New York University
**KELLY CAINE**, Clemson University
**RICHARD CHOW**, Intel Corporation
**PAUL ENGLAND (NAE)**, Independent Consultant
**ANDRÉ FREITAS**, University of Manchester, Idiap Research Institute, and Cancer Research UK Manchester Institute
**ALFIO GLIOZZO**, IBM Research
**GREGORY F. LAWLER (NAS)**, University of Chicago
**ANNA LYSYANSKAYA**, Brown University
**CHARIF MAHMOUDI**, Siemens
**LINDA R. PETZOLD (NAS/NAE)**, University of California, Santa Barbara
**MANAS N. RACHH**, Flatiron Institute
**JEYAVIJAYAN (JV) RAJENDRAN**, Texas A&M University
**DEBORAH SHANDS**, SRI International
**EUGENE H. SPAFFORD**, Purdue University
**SHENGTAO WANG**, QuEra Computing
**TOLGA YALCIN**, Qualcomm
**SHERALI ZEADALLY**, University of Kentucky
**MARY ELLEN (“MEZ”) ZURKO**, MIT Lincoln Laboratory

*Study Staff*

**KATIE BRATLIE**, Director, Laboratory Assessments Board
**JAMES MYSKA**, Senior Program Officer, *Study Director*
**MAURA WALSH**, Administrative Coordinator

Copyright National Academy of Sciences. All rights reserved.

## LABORATORY ASSESSMENTS BOARD

**TJ GLAUTHIER**, TJG Energy Associates, *Chair*
**ROBERT D. BRAUN (NAE)**, Johns Hopkins University Applied Physics Laboratory
**DAVID S.C. CHU**, Institute for Defense Analyses
**DONA L. CRAWFORD**, Lawrence Livermore National Laboratory (retired)
**THOMAS R. KURFESS**, Georgia Tech Manufacturing Research Institute
**JUAN DE PABLO (NAS/NAE)**, The University of Chicago
**CAROL SCHUTTE**, Air Force Office of Scientific Research (retired)

*Study Staff*

**KATIE BRATLIE**, Director
**LIZA RENEE HAMILTON**, Senior Program Officer
**JAMES MYSKA**, Senior Program Officer
**MAURA WALSH**, Administrative Coordinator

Copyright National Academy of Sciences. All rights reserved.

# 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:

**PETER BELING**, Virginia Polytechnic Institute and State University
**ELISA BERTINO**, Purdue University
**VINTON CERF (NAS/NAE)**, Google, LLC
**JAMES CURRY**, University of Colorado Boulder
**KAREN KAFADAR**, University of Virginia
**ELAINE PALMER**, IBM Research

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 **ELSA REICHMANIS (NAE)**, Lehigh University, and **DAVID W. JOHNSON, JR. (NAE)**, Bell Laboratories, Lucent Technologies. They were 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.

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

# Contents

APPENDIXES

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

# Summary

## BACKGROUND AND TASK

Since 1959, the National Institute of Standards and Technology (NIST) has annually solicited the National Academies of Sciences, Engineering, and Medicine to convene expert panels. These panels, comprising professionals from academia, industry, and other scientific and engineering fields, are tasked with evaluating the quality, effectiveness, and resource sufficiency of NIST's six measurement and standards laboratories. NIST engages the National Academies for these evaluations through an annual contract. For fiscal year 2024, NIST has requested that the National Academies evaluate its Information Technology Laboratory (ITL). As part of this assessment, the panel conducted a site visit, during which they toured the laboratory, held one-on-one discussions with ITL researchers, and followed up with additional inquiries. Leveraging their expertise, the panel reviewed ITL according to the defined scope of work and provided relevant recommendations.

The statement of task includes four key objectives. First, the panel is asked to evaluate ITL's technical programs, comparing the quality of its research to similar international initiatives and determining whether the programs are sufficient to achieve ITL's objectives. Second, the panel is asked to assess ITL's scientific and technical expertise portfolio, considering whether it is world-class and how well it supports ITL's programs and goals. Third, the panel must review the adequacy of ITL's facilities, equipment, and human resources in supporting its technical efforts and overarching mission. Last, the panel is asked to evaluate ITL's effectiveness in disseminating program outcomes, including how well these efforts address stakeholder needs, the comprehensiveness of its dissemination and technology transfer methods, and how effectively ITL monitors stakeholder use and the impact of its outputs.

## INFORMATION TECHNOLOGY LABORATORY

ITL comprises six divisions: the Applied and Computational Mathematics Division, the Applied Cybersecurity Division, the Computer Security Division, the Information Access Division, the Software and Systems Division, and the Statistical Engineering Division. These divisions are housed at the NIST campus in Gaithersburg, Maryland; the National Cybersecurity Center of Excellence (NCCoE) in Rockville, Maryland; and the NIST campus in Boulder, Colorado. These divisions contribute to the mission to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics" (NIST 2020). This report assesses the Applied and Computational Mathematics Division, the Applied Cybersecurity Division, and the Computer Security Division.

Copyright National Academy of Sciences. All rights reserved.

## OVERARCHING THEMES AND KEY RECOMMENDATIONS

### Strategic Direction and Strategic Planning

The panel noted that, despite impressive outcomes, ITL appears to need a more structured strategic plan, with new projects appearing to be driven primarily by legislation and executive orders. Concerns were raised about future staffing levels owing to potential retirements, which could spread available resources too thin and reduce ITL's ability to deliver broader and more impactful outcomes. Although some strategic vision was evident, it needs clearer and more systematic development and efficient collaborations both within and outside NIST. Developing a well-structured strategic plan would holistically align ITL's diverse projects with current and future trends, external demands, and emerging topics, helping to consolidate efforts and enable the efficient use of resources.

The panel also found that criteria for defining, prioritizing, and evaluating projects were sometimes not sufficiently clear, and ITL's overwhelming project demands and budget constraints limit its capacity for in-depth project work. Improved coordination, mentoring, and cross-group collaboration are needed to align projects with ITL's mission and optimize resource use.

> **Key Recommendation 1: The Information Technology Laboratory should create a structured strategic plan based on its overarching vision to concentrate its efforts and resources on the most critical areas of work. This will help avoid initiation of projects that are misaligned with the division's strategic goals and prevent the dilution of resources, ensuring greater impact.**

### Metrics and Stakeholder Relevance

The panel observed that ITL currently measures its accomplishments based on outputs such as the number of papers, patents, and meetings rather than on outcomes such as impacts on U.S. commerce, the economic scale of supported ecosystems, or the frequency of algorithm usage. Such outputs are easier to quantify but may not impress appropriators. ITL would benefit from focusing on and communicating the tangible impacts on U.S. industry and sharing industry use case stories with legislative staff. Similarly, for ITL's extensive support of federal agencies, collecting and sharing use case stories would be more effective in communicating impacts than merely reporting the number of publications.

The panel strongly believes the division's work appeals to a broader audience beyond its typical stakeholders. While ITL engages with NIST's Public Affairs Office, it is unclear whether current communication channels adequately highlight ITL's work to external stakeholders. Researchers engage with the academic community and the Department of Commerce, but a clear strategy for broader external communication could be impactful. Key questions to address include the following: Which stakeholders beyond the usual ones should ITL's work reach (e.g., Congress, industry, education, or citizens)? What positive outcomes could arise from broader engagement (e.g., increased funding or better access to resources)? What are the most effective communication channels (e.g., events, videos, textual content)? What is ITL's web presence strategy, and what resources are needed to optimize communication outcomes?

ITL's current communication channels may not effectively reach external stakeholders. The panel suggests improving visibility to various communities (e.g., Congress, industry, academia) and enhancing communication strategies, including web presence. Additionally, while dissemination metrics focus on reach, there is a need for metrics that measure and communicate impact to stakeholders and appropriators and for these metrics to be included in the strategic plan.

ITL needs to develop metrics that better assess and communicate the impact of its projects to stakeholders and appropriators. Considering constraints on surveying stakeholders, ITL might explore alternative metrics, such as tracking external contributions to ITL documents or reported issues by adopters. Ideas from the open-source community, like those outlined in the Linux Foundation's

Copyright National Academy of Sciences. All rights reserved.

"Measuring Your Open Source Program's Success," could be useful.[1] Additionally, measuring the percentage of repeat collaborating companies could indicate industry value, with different implications for small start-ups versus large technology firms. Years ago, NIST did contract some NIST impact studies (NIST 2023). These studies might be a useful template for ITL to measure impact.

**Key Recommendation 2: The Information Technology Laboratory (ITL) should develop impact metrics to be applied uniformly across all of its work. Metrics should, whenever possible, include both the economic benefits for adopters and measurable reductions in risk. These metrics should illustrate the impacts and outcomes of ITL's work rather than simply providing outputs. Plans for improved communication with ITL's current and potential stakeholders should be included in the strategic plan.**

## Artificial Intelligence

The panel believes that artificial intelligence (AI) will significantly impact ITL's work, with potential opportunities that include the use of large language models for scientific and mathematical discovery and enhancing these models. It is advisable that ITL develop a more ambitious AI strategy focused on critical infrastructures, tools, and methods, and identify key areas for national and international leadership.

Recent advancements in foundational AI and its applications have been revolutionary, and AI is expected to affect nearly all aspects of life and commerce in the coming years. However, its impact on computer security remains uncertain. AI can be used by both attackers and defenders, and the introduction of new AI-driven products and services will bring risks that are not yet fully understood. Additionally, there are growing privacy concerns surrounding the data used to train AI systems. All of this suggests tremendous technological opportunities for ITL.

The panel emphasizes that for ITL to remain effective over the next decade, it must invest in AI staffing, equipment, and expertise. While hiring permanent staff is a long-term solution, establishing a contractor-based or visiting researcher program could be a practical short-term arrangement to enable more agile knowledge transfer. This approach would allow the division to swiftly explore how contemporary AI techniques, such as large language models, can be integrated into existing research workflows. Such contractors and visiting researchers can also be a source for new ITL employees over time.

Cutting-edge research, model training, and AI inference require substantial investment in hardware, data, software, operational resources (such as power), and staff. Building these capabilities will be costly, and attracting top talent will depend on ensuring adequate facilities.

**Key Recommendation 3: The Information Technology Laboratory should enhance its artificial intelligence (AI) expertise to continue being able to have significant impacts in this area. In the long term, this will require adding AI researchers and engineers, either by hiring new talent or by upskilling current staff, or a combination of both. In addition to building a permanent team, the division can create a contractor or visiting researcher program to facilitate flexible knowledge transfer in AI. Such initiatives could also help identify potential candidates for future hiring.**

[1] The Linux Foundation's Open Source Guide "Measuring Your Open Source Program's Success" can be found at https://www.linuxfoundation.org/resources/open-source-guides/measuring-your-open-source-program-success, accessed August 21, 2024.

Copyright National Academy of Sciences. All rights reserved.

## REFERENCES

NIST (National Institute of Standards and Technology). 2020. “ITL Mission.” Information Technology Laboratory. https://www.nist.gov/itl/about-itl/itl-mission.

NIST. 2023. “Summary of NIST Impact Study Results.” Updated August 23. https://www.nist.gov/tpo/summary-nist-impact-study-results.

Copyright National Academy of Sciences. All rights reserved.

# 1
# Introduction

## STATEMENT OF TASK

Starting in 1959, the National Academies of Sciences, Engineering, and Medicine have 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 six National Institute of Standards and Technology (NIST) measurements and standards laboratories,[1] as well as the adequacy of the laboratories' resources. These reviews are conducted under contract at the request of NIST.

For fiscal year (FY) 2024, NIST looks forward to the panel's review of the Information Technology Laboratory (ITL). The assessment of ITL will address the following factors at the request of the NIST Director:

1. Assess the organization's technical programs.
   - How does the quality of the research compare to similar world-class research in the technical program areas?
   - ls the quality of the technical programs adequate for the organization to reach its stated technical objectives? How could it be improved?
2. Assess the portfolio of scientific expertise within the organization.
   - Does the organization have world-class scientific expertise in the areas of the organization's mission and program objectives? If not, in what areas should it be improved?
   - How well does the organization's scientific expertise support the organization's technical programs and the organization's ability to achieve its stated objectives?
3. Assess the adequacy of the organization's facilities, equipment, and human resources.
   - How well do the facilities, equipment, and human resources support the organization's technical programs and its ability to achieve its stated objectives? How could they be improved?
4. Assess the effectiveness by which the organization disseminates its program outputs.
   - How well are the organization's research programs driven by stakeholder needs?
   - How effective are the dissemination methods and technology transfer mechanisms used by the organization? Are these mechanisms sufficiently comprehensive?
   - How well is this organization monitoring stakeholder use and impact of program outputs? How could this be improved?

## CONDUCT OF THE ASSESSMENT

The overall structure of ITL, its goals, and the associated programs are described in Chapter 2. This report assesses three of ITL's divisions:

[1] The six NIST laboratories are the Center for Neutron Research, Communications Technology Laboratory, Engineering Laboratory, Information Technology Laboratory, Material Measurement Laboratory, and Physical Measurement Laboratory.

Copyright National Academy of Sciences. All rights reserved.

- Applied Cybersecurity Division (ACD)
- Applied and Computational Mathematics Division (ACMD)
- Computer Security Division (CSD)

The panel held a meeting and site visit on June 4–6, 2024, in Gaithersburg, Maryland. At this meeting, the panel as a whole received an introductory overview of NIST and ITL. The panel then broke into three separate subpanels that met independently and in parallel with the ITL staff aligned with the divisions assessed in this report. These subpanel meetings included structured presentations, discussions, and tours. The panel as a whole also had a working lunch with early career ITL staff and postdoctoral researchers.

## STRUCTURE OF THIS REPORT

This report opens with this introductory chapter, followed by an overview of ITL. Each ITL division assessed in this report is then presented in its own chapter. The structure within each of these chapters is aligned with the statement of task presented above to aid the reader in understanding the panel's assessment. Following the assessment chapters is a chapter that presents selected recommendations from the FY 2018 and FY 2021 ITL assessment reports—the last time these divisions were assessed—and ITL's responses to those recommendations. The final chapter presents the recommendations from the current report in one place for ease of reference. The structure of this report is laid out thus:

- Chapter 1: Introduction
- Chapter 2: Overview of the Information Technology Laboratory
- Chapter 3: Applied Cybersecurity Division
- Chapter 4: Applied and Computational Mathematics Division
- Chapter 5: Computer Security Division
- Chapter 6: Information Technology Laboratory's Responses to the Recommendations of Previous Assessment Reports
- Chapter 7: Overarching Themes, Key Recommendations, and Chapter Recommendations

To draft this report, the panel reviewed the material provided by ITL before and during the review meeting. ITL chose what information to provide to the panel. The panel applied a largely qualitative approach to the assessment, using the members' professional experience, expertise, and judgment to conduct the assessment. The panel was quantitative where possible, but much of this assessment is, by its nature, subjective, and the panel's opinions are based on the facts presented to it.

Because this assessment depends on the information presented by ITL, it is not exhaustive. Similarly, there are natural variations among the assessment chapters (Chapters 3–5) in terms of length, level of detail, and approach. These convey no message about the quality of work being performed by ITL or the information provided to the panel. Each assessment chapter was drafted by one of the subpanels and reflects the content that the ITL staff chose to present to each subpanel and the level of detail provided to that subpanel. The assessment chapters are also not a comprehensive presentation of the entirety of the information provided to the subpanels. Rather, each subpanel selected what stood out to its members in fulfillment of its statement of task and drafted the chapter around those items. Thus, the omission in this report of any particular ITL project is not a negative reflection of the omitted project.

Last, the statement of task asks in some places if the work of ITL is "world-class" or how it compares with work at other international institutes. This is always a subjective assessment based on the totality of the panelists' knowledge and experience. No comprehensive picture of work around the world

Copyright National Academy of Sciences. All rights reserved.

was compiled; there was no time for it. Also, in many instances, NIST's work is unique in the world. This, itself, makes much of the work world-class or world-leading.

## USE OF THE 2023 NIST *CAPITAL FACILITY NEEDS* REPORT IN THE PANEL'S WORK

This report adopts the full description of the problems identified in *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology* (NASEM 2023). Box 1-1 summarizes that report and its findings and recommendations.

### BOX 1-1
### *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology*

In February 2023, the National Academies of Sciences, Engineering, and Medicine released the report *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology* (NASEM 2023; hereafter, the *Capital Facility Needs* report). The committee that authored this report was tasked with assessing the National Institute of Standards and Technology's (NIST's) facilities and utility infrastructure, and reviewing and assessing plans and projects to reinvigorate NIST's facilities and utility infrastructure, the cost estimates for doing so, and the factors that NIST should consider in developing a comprehensive capital strategy for the facilities and utility infrastructure at NIST's campuses in Boulder, Colorado, and Gaithersburg, Maryland. The committee engaged with the Department of the Interior, the National Institutes of Health, the U.S. Army Engineer Research and Development Center, and the Johns Hopkins University Applied Physics Laboratory to learn about their methods and metrics for assessing facility conditions and maintaining their facilities.

The condition of NIST's facilities and utility infrastructure has been a concern since 2002, when the Visiting Committee on Advanced Technology (VCAT) issued a report calling NIST's facilities condition and the related funding situation "alarming" and "critical." Over the following 20 years, the VCAT returned consistently to this theme with increasingly dire language. Eventually, the conference report accompanying the Consolidated Appropriations Act of 2021 (P.L. 116-260) requested that NIST "contract with an independent entity to develop a report that assesses the comprehensive capital needs of NIST's campuses." In response, NIST's Office of Facilities and Property Management approached the National Academies to conduct a study based on a successful study and report completed for the National Institutes of Health in 2019 (NASEM 2019). The result was the *Capital Facility Needs* report (NASEM 2023).

The committee that authored the *Capital Facility Needs* report visited both the Boulder, Colorado, and the Gaithersburg, Maryland, campuses. It discovered that many NIST facilities are inadequate to support the world-leading research that is NIST's mission. Both the quality and the reliability of power can be problematic, resulting in slowed work, lost work, and unnecessary time spent recalibrating sensitive instruments. Inadequacies in basic environmental controls can result in laboratories that are too hot or cold, too humid, or not humid enough, and lack proper vibration insulation. In one 1950s-era Boulder laboratory, the gaps between the windows and frames allow dust to blow straight into the laboratory. Roof leaks have destroyed multimillion-dollar pieces of equipment, such as tunneling electron microscopes in both Boulder and Gaithersburg. A water leak in Gaithersburg resulted in permanent damage to the world-leading Kibble balance that tied the standard kilogram to the speed of light. There are many more instances and stories. In all, the committee found that the NIST research staff loses 10–40 percent of its working time fighting against facility inadequacies, also consuming research money to do so. Conditions have reached the point where NIST researchers will not be able to continue their world-class research no matter their efforts. This is already impacting the ability to recruit and retain staff and the willingness of foreign researchers to do work at NIST. At risk also is NIST's international credibility and influence and its ability to support national security, U.S. international competitiveness, medical therapeutics, and a wide range of other activities on which users in the U.S. government, industry, and academia rely.

Copyright National Academy of Sciences. All rights reserved.

**TABLE 1-1-1** Overview of NIST Facility and Infrastructure Funding Needs

| Funding Component | Amount Needed Annually |
|---|---|
| Construction and major renovations (CMR) | $300 million to $400 million |
| Safety, capacity, maintenance, and major repairs (SCMMR) | $120 million to $150 million |
| Total needed for construction of research facilities (CRF) | $420 million to $550 million |

NOTE: CRF funding is the sum of CMR and SCMMR funding.
SOURCE: NIST (2022).

In the course of its work, the committee found that NIST's internal facility and property management policies are not responsible for this situation. Rather, the cause is more than 2 decades of erratic, unpredictable, and inadequate funding for NIST's construction of research facilities budget, which includes facility sustainment, restoration, modernization, and expansion. Exacerbating this problem is congressionally directed pass-through funding for items such as building laboratories on university campuses that are not used by NIST. This pass-through funding is not revenue-neutral to NIST, costing staff time and money to administer, draining even more much-needed money from NIST's facilities coffers.

In short, the committee found that the situation requires serious and sustained attention, particularly from leadership levels above NIST. The committee also endorsed the coordinated recovery plan drafted by NIST's Office of Facilities and Property Management and recommended its continued refinement and shortening its timeline to completion in 12 years. Critically, the committee identified the need for significant and sustained funding to address NIST's facilities and utility shortcomings and bring them to the standard necessary for modern metrology. This funding is the critical piece of the recovery plan. The committee recommends $420 million–$550 million per year in funding for NIST's construction of research facilities budget over at least 12 years. As shown in Table 1-1-1, this includes $120 million–$150 million per year for safety, capacity, maintenance, and major repairs funding to address the more than $800 million deferred maintenance backlog and to bring existing facilities to an acceptable condition and keep them there. It also includes $300 million–$400 million per year over at least 12 years for the construction and major renovations budget to upgrade, renovate, and build the new laboratories with the new capabilities needed to conduct modern metrology research.

The picture is not unremittingly bleak. NIST has already begun to modernize laboratories as its current budget allows. These new laboratories are state of the art and enable the cutting-edge world-leading research that is NIST's mission. As an example, one NIST research group—after waiting 18 months to be relocated into a new, modern laboratory—won the 2021 Physics World Breakthrough of the Year award for a previously unprecedented demonstration of the quantum entanglement of microresonators. NIST's staff is world-class and capable of producing amazing results, results that will serve the nation and inspire the next generations of researchers, provided they are given the facilities and tools needed to do their work.

SOURCE: NASEM (2023).

## REFERENCES

NASEM (National Academies of Sciences, Engineering, and Medicine). 2019. *Managing the NIH Bethesda Campus Capital Assets for Success in a Highly Competitive Global Biomedical Research Environment*. The National Academies Press. https://doi.org/10.17226/25483.

NASEM. 2023. *Technical Assessment of the Capital Facility Needs of the National Institute of Standards and Technology*. The National Academies Press. https://doi.org/10.17226/26684.

NIST (National Institute of Standards and Technology). 2022. "NIST Facilities Summary for Representative Trone." Point Paper. June. Office of Facilities and Property Management.

Copyright National Academy of Sciences. All rights reserved.

# 2
# Overview of the Information Technology Laboratory

The Information Technology Laboratory (ITL) is one of the National Institute of Standards and Technology's (NIST's) six major laboratories.[1] ITL describes its purpose as being "to cultivate trust in information technology (IT) and metrology," with "the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics" (NIST 2020).

ITL is located at the NIST campus in Gaithersburg, Maryland; the National Cybersecurity Center of Excellence (NCCoE) in Rockville, Maryland; and the NIST campus in Boulder, Colorado. Its facilities include NCCoE, an Immersive Visualization Laboratory, a Biometrics Research Laboratory, and a Usability Testing Laboratory.

ITL is organized into six divisions:

- Applied and Computational Mathematics Division
- Applied Cybersecurity Division
- Computer Security Division
- Information Access Division
- Software and Systems Division
- Statistical Engineering Division

The *Applied and Computational Mathematics Division* develops mathematical and computational techniques and tools with wide applicability. This division's work includes research in micromagnetic modeling; creating a digital library of mathematical functions; advanced data analysis for diagnostics, biometrology, and COVID-19; and the development of a standard reference mortar for use in building materials.

The *Applied Cybersecurity Division* establishes cybersecurity standards and guidelines openly, transparently, and collaboratively. It also practically applies NIST's research, standards, testing, and measurement to cybersecurity. The division's work includes the Cybersecurity Framework, the NICE Workforce Framework for Cybersecurity, used for cybersecurity education and workforce development, the Privacy Framework, and the NIST Cybersecurity for Internet of Things (IoT) Program.

The *Computer Security Division* protects federal IT systems with a suite of cybersecurity standards, guidelines, tests, and metrics. Its research is focused on cryptography, automation, identity and access management, the IoT, and public safety networks. The division's work includes post-quantum cryptography and security testing, validation, and measurement, and it maintains a National Vulnerability Database. It has a Computer Security Resource Center that provides access to the entire body of NIST's cybersecurity and information security-related projects, publications, news, and events.

The *Information Access Division* conducts research in the application of artificial intelligence (AI) in human language technologies, biometrics, search, information retrieval, and natural language processing. The division's work includes related measurement science, novel paradigms to evaluate

[1] The other five laboratories are the Center for Neutron Research, Communications Technology Laboratory, Engineering Laboratory, Material Measurement Laboratory, and Physical Measurement Laboratory.

Copyright National Academy of Sciences. All rights reserved.

technologies, and research to ensure that technology is developed and used correctly and efficiently. It includes a Multimodal Information Group, a Retrieval Group, an Image Group, and a Visualization and Usability Group.

The *Software and Systems Division* accelerates the development and adoption of correct, reliable, and testable software and information exchange standards. It develops rigorous techniques to evaluate software, which increases trust and confidence in software that is deployed across the nation and around the world. The division contributes to developing computationally enabled measurements with trust in computing and handling of high-throughput instruments built in by design. It has projects in software and quality assurance, the Configurable Data Curation System, image and text analytics, smart and connected systems, scalable systems, voting security, test methods using information technology for health and medical device applications, digital forensics, trojans in AI, category theory, cloud computing, digital twins, and timing.

The *Statistical Engineering Division* works to characterize measurement uncertainty, conduct foundational statistics research, and implement methods and techniques for experimental design, data analysis, statistical modeling, and probabilistic inference in computer software. The division publishes technical and educational materials in print and online, offering training courses and workshops and participating in professional conferences. The division conducts fundamental and applied statistical research on problems in metrology. It collaborates with other ITL divisions, other NIST laboratories, and industrial partners.[2]

This report focuses on the Applied Cybersecurity Division, the Applied and Computational Mathematics Division, and the Computer Security Division. The chapters assessing these divisions will contain information on budget, staff, and facilities specific to these divisions. Some information about ITL as a whole follows here.

## BUDGET

Figure 2-1 shows ITL's budget from fiscal year (FY) 2015 through FY 2024. The budget has increased from approximately $150 million in FY 2015 to approximately $180 million in FY 2024. ITL's budget comes from both external and internal funding. The external funding comprises congressional scientific and technical research services appropriations and reimbursable work for other federal agencies. It also included funding from the Public Safety Trust Fund until that fund expired in FY 2022. Internal funding, which is awarded competitively within NIST, comes through the Strategic and Emerging Research Initiatives program, the Innovations in Measurement Sciences program, and an assortment of other internal funding competitions.

Figure 2-2 shows ITL's labor costs for full-time equivalents (FTEs) from FY 2018 through FY 2024. A clear trend of rising labor costs is visible. The labor cost for FY 2024 is so low because it shows labor costs only from October 1, 2023, through May 31, 2024.

[2] The National Institute of Standards and Technology document "National Academies of Sciences, Engineering, and Medicine: Information Technology Laboratory Assessment 2024 Read-Ahead Materials" was obtained by the panel from NIST on June 23, 2024, and is available in the public access file for this study (Email: paro@nas.edu).

Copyright National Academy of Sciences. All rights reserved.

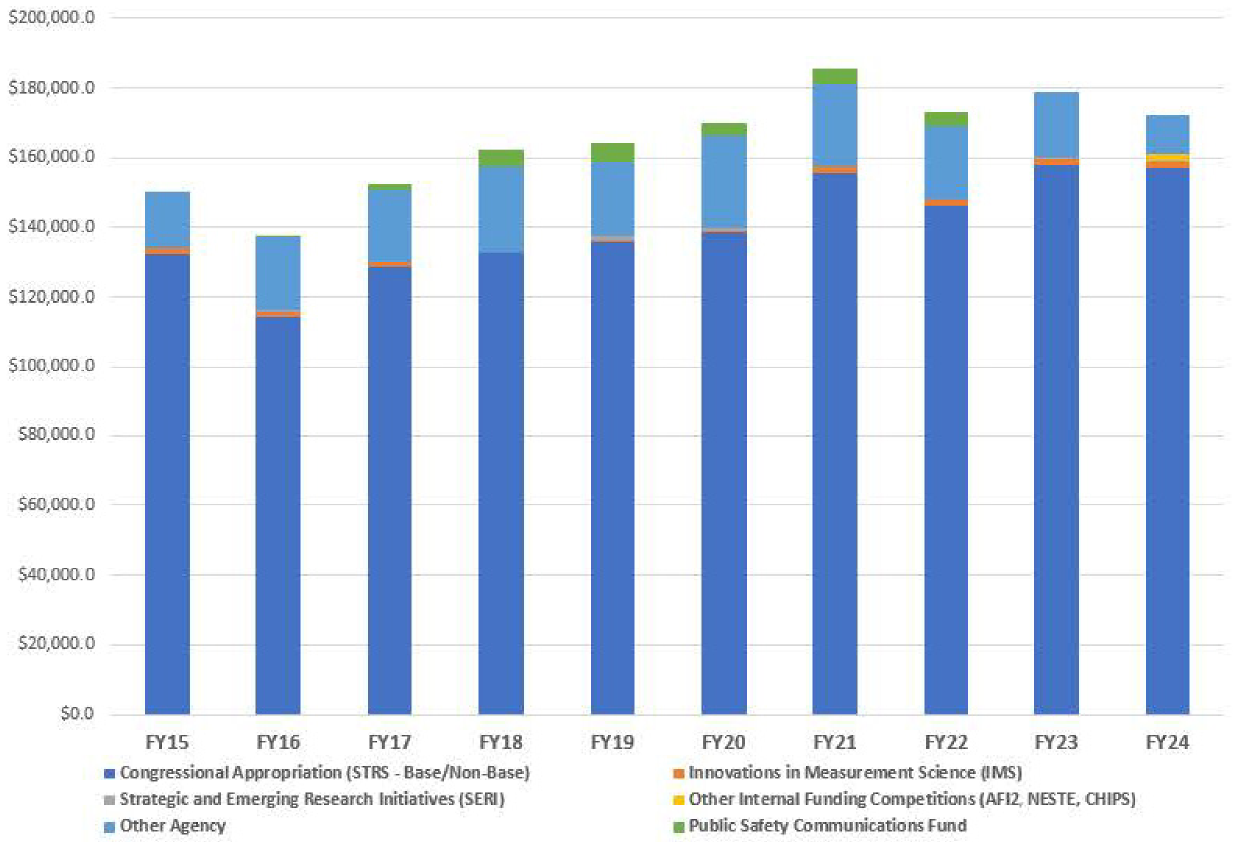


**FIGURE 2-1** Information Technology Laboratory budget from fiscal year (FY) 2015 through FY 2024.
NOTES: The Public Safety Communications Fund was formally known as the Public Safety Trust Fund. AFI2, Accelerating Forensic Innovation for Impact; CHIPS, CHIPS and Science Act of 2022; NESTE, NIST Emerging Technology Standards Engagement Pilot Program; STRS, scientific and technical research services.
SOURCE: Courtesy of NIST Information Technology Laboratory.

ITL also has an initiative named Building the Future. This initiative was founded in 2014. It is future-looking and intended to foster the exploration of the emerging needs of ITL stakeholders. This initiative does not support work that is only an extension or an incremental improvement. Successful projects under this initiative identify new competencies to support ITL's mission. Teams can be collaborative, but the lead must be a federal employee. Awards are as follows:

- *Seeker Awards:* These are small exploratory projects to identify new technologies that ITL may want to work with in the future.
- *Early Stage Research Awards:* These are small to midscale projects that conduct fundamental research to lay the foundations for ITL's measurement science work.
- *Research Awards:* These are larger projects aimed at building ITL's capacity—in terms of expertise and capabilities—in research areas that have already been identified for future exploration and work.

Figure 2-3 shows the number of proposals, awards, and funding under the Building the Future initiative from its founding in 2014 through the time of the panel meeting in June 2024.

Copyright National Academy of Sciences. All rights reserved.

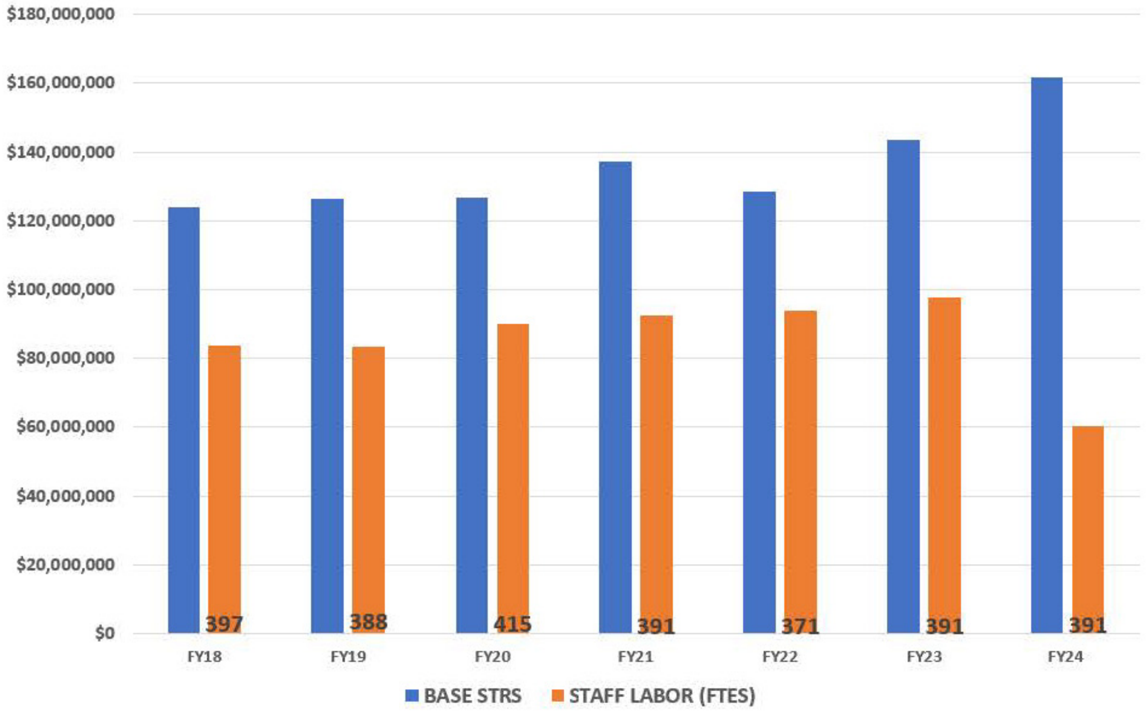
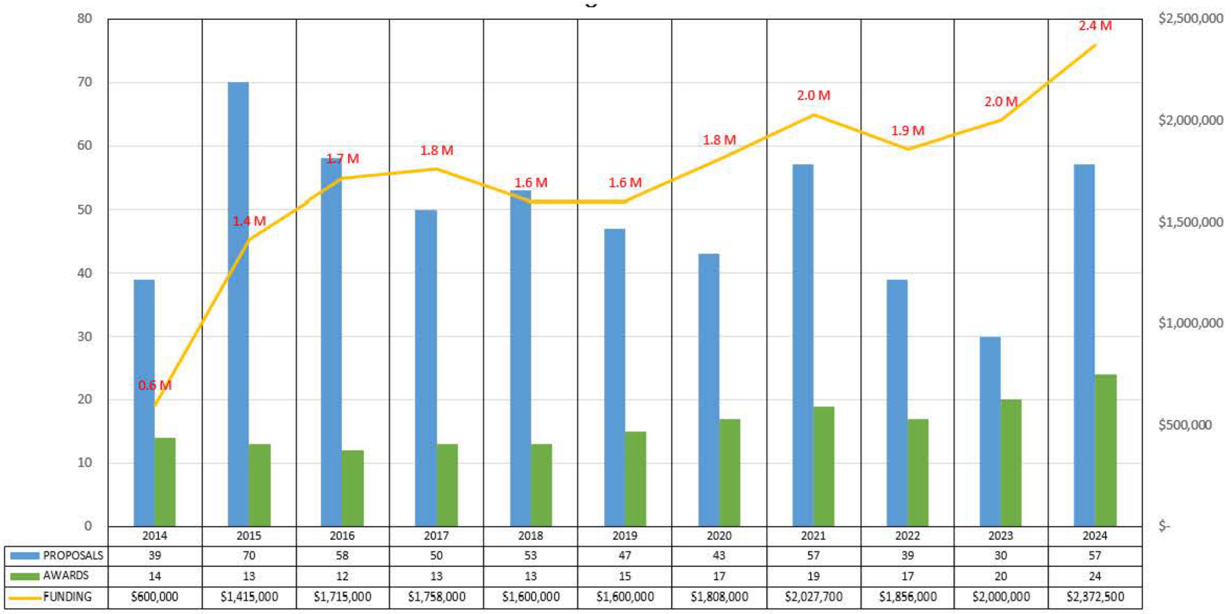


**FIGURE 2-2** Information Technology Laboratory labor costs for full-time equivalents (FTEs) compared with base scientific and technical research services (STRS) appropriations. Fiscal year (FY) 2024 shows only through May 31, 2024.
SOURCE: Courtesy of NIST Information Technology Laboratory.



| | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROPOSALS | 39 | 70 | 58 | 50 | 53 | 47 | 43 | 57 | 39 | 30 | 57 |
| AWARDS | 14 | 13 | 12 | 13 | 13 | 15 | 17 | 19 | 17 | 20 | 24 |
| FUNDING | $600,000 | $1,415,000 | $1,715,000 | $1,758,000 | $1,600,000 | $1,600,000 | $1,808,000 | $2,027,700 | $1,856,000 | $2,000,000 | $2,372,500 |

**FIGURE 2-3** Proposals, awards, and funding under the Building the Future initiative from its inception in 2014 through part of 2024. The left side shows the scale for the number of proposals and awards; the right side shows the scale for funding.
SOURCE: Courtesy of NIST Information Technology Laboratory.

Copyright National Academy of Sciences. All rights reserved.

**TABLE 2-1** Projected Retirement Eligibility Across the Information Technology Laboratory and the Divisions Assessed in This Report as of March 2024

| | Eligibility Over Time (Percent) | | | | |
|---|---|---|---|---|---|
| ITL Area | Now | Within 3 Years | Within 5 Years | Within 10 Years | More Than 10 Years |
| ITL overall | 34 | 9 | 5 | 9 | 43 |
| ACMD | 42.3 | 5.8 | 3.8 | 11.5 | 36.5 |
| CSD | 32 | 15 | 6 | 10 | 37 |
| ACD | 26.1 | 6.5 | 2.2 | 8.7 | 56.5 |

NOTE: ACD, Applied Cybersecurity Division; ACMD, Applied and Computational Mathematics Division; CSD, Computer Security Division; ITL, Information Technology Laboratory.
SOURCE: Data courtesy of NIST Information Technology Laboratory.

## STAFF

ITL has 689 staff in total: 393 are federal employees, 159 are contractors, 89 are guest researchers, and 48 fall into an "other" category that includes people such as postdoctoral researchers and students. Of these ITL staff members, 67 work remotely in 22 states and the District of Columbia. ITL's personnel policies encompass telework and remote work, culture, safety, recruitment and retention, facilities and infrastructure for research computing, and faculty annuitants and foreign guest researchers. Of the job candidates across all areas referred to ITL since May 2021, 48 percent have been minorities, with the proportion of minority staff increasing from 25 percent in 2021 to 28 percent in 2024. Also since May 2021, 50 percent of ITL's new hires have been women, and the proportion of female staff has increased from 34 percent in 2021 to 38 percent in 2024.

A significant proportion of ITL's staff is eligible for retirement now and within the next 10 years. The data across ITL and broken out for the divisions assessed in this report are shown in Table 2-1.

## PARTNERSHIPS, COLLABORATIONS, AND REACH

ITL has a number of partnerships and collaborations with industry and academia. These include NCCoE partners, communities of interest, cooperative research and development agreements, and working with the AI Safety Institute Consortium, Joint Center for Quantum Information and Computer Science, Washington Metropolitan Quantum Network Research Consortium, and Trustworthy AI in Law and Society. ITL also engages in interagency work with, for example, the Department of Homeland Security, National Security Agency, Intelligence Advanced Research Projects Activity, Federal Bureau of Investigation, National Science Foundation, and Department of State, and others.

Metrics of ITL's reach from FY 2021 through FY 2023 include

- A growth of about 30,000 social media followers, from approximately 38,000 to approximately 68,000
- 45 blogs with approximately 95,000 views
- About 152 million unique visits to ITL websites
- Hosting more than 160 conferences and events—in-person, hybrid, and remote—with more than 55,000 total registrants
- 206 technical series publications with more than 3.1 million downloads

Copyright National Academy of Sciences. All rights reserved.

- 149 journal articles
- 132 conference papers

## REFERENCE

NIST (National Institute of Standards and Technology). 2020. "Information Technology Laboratory: ITL Purpose." https://www.nist.gov/itl/about-itl/itl-purpose.

Copyright National Academy of Sciences. All rights reserved.

# 3
# Applied Cybersecurity Division

## INTRODUCTION

The Applied Cybersecurity Division (ACD) of the Information Technology Laboratory (ITL) was established on October 1, 2015. ACD's mission is to "implement practical cybersecurity and privacy through outreach and effective application of standards, guidelines, and best practices necessary for the U.S. to adopt cybersecurity and privacy capabilities" (Stine and Petersen 2024).

Outreach to industry, academia, government, and others is central to ACD's work. An important part of the outreach is listening to the needs and desires of its stakeholders. This ensures that the division focuses on the most important problems and builds trust, leading to increased influence.

The division approaches the task of ensuring that standards and guidance are applied effectively primarily through the National Cybersecurity Center of Excellence (NCCoE), which is a collaborative hub for government, industry, and academia to work together on pressing cybersecurity and privacy issues. ACD also devotes significant resources to ensuring that National Institute of Standards and Technology (NIST) guidance and specifications on privacy and security are effective through their Cybersecurity and Privacy Frameworks programs. Other NCCoE programs include the development and study of 5G deployments, digital identities (including mobile driver's licenses), election systems, and the transition to post-quantum cryptography.

Education and workforce needs are addressed through the National Initiative for Cybersecurity Education (now known simply as NICE). NICE is also effective in developing the job market for cybersecurity researchers and practitioners by promoting a common language for skills and learning.

The Internet of Things (IoT) is a fast-moving technology area with concomitant security risks. ACD is active in enabling the deployment of secure and privacy-sensitive IoT devices by developing guidelines and requirements for the procurement and use of IoT devices across the federal government. The NIST Cybersecurity for IoT team also works to harmonize guidance and requirements across the globe by working with European Union regulators.

Other ACD activities include education and support for small businesses to benefit from NIST specifications and guidance.

ACD is central to driving changes to cybersecurity standards and practice. The division advances standards and guidelines critical to protecting the cyber infrastructure of the public and private sectors. The goal is to drive greater adoption of viable and widely adopted cybersecurity standards. ACD meets a critical need in cybersecurity by educating the cybersecurity workforce. It enables national and international consensus using public and private partnerships. Notably, ACD advances the market position of U.S. companies; the U.S. industry derives enormous benefits from the efforts of ACD, ITL, and NIST. ACD is critical to developing and driving changes to cybersecurity standards in the United States and globally.

Not every project presented to the panel is discussed in this report. Only those projects about which the panel had comments are discussed.

Copyright National Academy of Sciences. All rights reserved.

## ASSESSMENT OF TECHNICAL PROGRAMS

### National Cybersecurity Center of Excellence

NCCoE operates a collaborative hub to engage industry, government agencies, and academic institutions to accelerate the adoption of cybersecurity technologies. With its collaborators, NCCoE prototypes cybersecurity solutions for profiled environments using commercially available technology configured according to standards and best practice guidelines. NCCoE's cybersecurity prototype solutions (1) enable the assessment of the practicality of implemented standards and guidelines and (2) facilitate their improvement.

NCCoE is currently pursuing 21 projects in the areas of risk management, applied cryptography, trusted platforms, operational technology, digital identity, and emerging technologies. NCCoE is addressing challenging problems throughout its portfolio of practical cybersecurity projects. The panel was introduced to 6 of the 21 projects, which are reviewed here. A review of the non-NCCoE projects follows the NCCoE projects.

### NCCoE Migration to Post-Quantum Cryptography Project

The publication of Shor's algorithm in 1994 suggested that many of the then-current encryption algorithms would be easily breakable with the advent of working quantum computers. The development pace of quantum technologies since that time suggests that the development of working quantum systems may be only 1 or 2 decades away. Not only is this a threat to ongoing cryptographic methods, but it also poses a threat to encrypted communications and data that may be stolen and held by malicious actors until technology resistant to quantum code-breaking is available—that is, encrypted data may be valuable to malicious actors even if it is not decrypted for decades.

It is critical that users of cryptography protect important material (e.g., health records, financial systems, and valuable intellectual property) by switching to quantum-resistant methods as soon as possible, to be ready to protect current data against future attacks when (and if) workable quantum computing is available to break cryptography. However, it takes time to make such a switch: to identify all of the use cases that need to be changed; introduce workable, tested methods; and ensure compatibility among products. This process may take years to complete, especially in large commercial products and databases.

NIST began an effort in 2016 to define new quantum-resistant algorithms for cryptographic use. This has been conducted in an open, collaborative mode with experts around the world. Candidate standards were published in 2021, and the first standards were published this year. To prepare for the release of official standards, NCCoE established an effort to coordinate and facilitate the switchover to quantum-resistant cryptography. This has included work on documentation, discovery tools, process models, and metrics.

### NCCoE 5G Security Standards and Applied Research and the Zero Trust Laboratory Project

ACD has collaborated with industry stakeholders and academic institutions to establish a laboratory to design cybersecurity solutions tailored to 5G. This project focuses on integrating advanced technologies such as Network Functions Virtualization and Software-Defined Networking. It emphasizes a holistic approach that combines these technologies with cloud-based security features outside the scope of the 3rd Generation Partnership Project 5G security architecture, resulting in a robust security reference architecture.

Key project areas include secure network architecture, secure software development, and advanced threat detection and response mechanisms. The project highlights zero-trust principles, ensuring continuous monitoring and verification of network components. It also addresses supply chain security, recommending practices such as using static and dynamic analysis tools to identify vulnerabilities and

Copyright National Academy of Sciences. All rights reserved.

implementing secure update mechanisms to protect software and hardware components. Advanced threat detection capabilities are a critical focus to analyze network traffic and detect anomalies in real time. By integrating these technologies with 5G core network functions such as the Access and Mobility Management Function and User Plane Function, the project enhances the network operator's ability to respond to security incidents promptly.

Additionally, the project explores the security implications of network slicing, a key feature of 5G that allows multiple virtual networks to operate on shared physical infrastructure. It provides guidelines for isolating and securing individual network slices to prevent the lateral movement of threats and ensure data confidentiality and integrity.

The project collaborates with various industry partners, including Dell Technologies, Intel, and Nokia. These organizations contribute relevant capabilities and product components to build and validate the example solutions. The project's standards engagements are also critical. The technical outputs and insights gained from ACD's research efforts form the foundation for active participation and contributions to the development of next-generation (e.g., 6G) cellular security standards. This ensures that the knowledge and advancements made by the project influence and shape future security protocols and guidelines in the 5G domain.

### NCCoE Zero Trust Project

The Zero Trust project is intended to establish practical and actionable guidelines for implementing zero-trust principles within enterprise environments. This project seeks to address the ever-changing cybersecurity landscape. Historically, cybersecurity has been based on perimeter defenses, keeping people out. This approach is no longer adequate to protect against ever more sophisticated threats. Zero-trust architecture fundamentally shifts the security paradigm by assuming that threats could exist both inside and outside the network, and therefore, every access request should be authenticated, authorized, and continuously validated.

The Zero Trust project is structured around a collaborative effort involving industry experts, government agencies, and academic institutions. This consortium seeks to develop reference architectures and implementable solutions that enterprises can use to enhance their cybersecurity posture. By leveraging existing technologies and integrating them into a cohesive framework, the project provides practical examples and use cases demonstrating the application of zero-trust principles. These include identity and access management, micro-segmentation, continuous monitoring, and analytics to detect and respond to anomalies.

A key component of the project is the creation of detailed practice guides that outline the steps required to implement zero-trust architecture in various scenarios. These guides cover the configuration of technologies such as multifactor authentication, endpoint security, encryption, and network infrastructure. By providing a comprehensive and modular approach, ACD seeks to make zero-trust adoption feasible for organizations of different sizes and sectors, addressing common challenges such as legacy systems integration and scalability.

### NCCoE Mobile Driver's License Project

The Mobile Driver's License project is new and is currently seeking collaborators. The project team described their first proposed use case focused on the use of a mobile (digital) driver's license in a "know your customer" process for a financial services institution. This project will deploy technologies involved in identity verification and authentication and will apply standards addressing credential syntax and semantics, credential presentation protocols and application programming interfaces, and identity management.

While the project will begin with use cases for a mobile driver's license, the project team intends to expand the scope of the project in the future to evaluate the use of other forms of verifiable identity credentials, such as the World Wide Web Consortium's Verifiable Credentials.

Copyright National Academy of Sciences. All rights reserved.

This project is important, is well thought through, and is a good use of NCCoE's limited resources. The panel strongly agrees with the project team's intent to expand the testbed and use cases to assess other forms of verifiable identity credentials.

### NCCoE NIST Cybersecurity Framework Profiles Project

The Cybersecurity Framework 2.0 introduces Community Profiles, which provide tailored cybersecurity risk management guidance for groups of organizations with common priorities. Community Profiles serve as collective cybersecurity risk management guidance for communities organized around the Cybersecurity Framework's common taxonomy. They differ from Organizational Profiles, which are not shared publicly. The ACD team offers a structured approach to creating these profiles, including a template and a life-cycle model. By following the appropriate life-cycle model and leveraging the shared expertise within communities, organizations can enhance their cybersecurity posture.

### NCCoE Cybersecurity and Privacy for Genomic Data Processing Project

Low-cost genomic sequencing has led to the creation of huge amounts of data, which contributes to U.S. leadership in health care. Genomic data need to be collected into large data sets to provide optimal value, but this aggregation leads to significant security and privacy risks. Privacy risks include leaks of people's data. Security risks include the disclosure of proprietary data sets to competitors. An extreme example of a threat would be the use of such data sets to develop bioweapons (as noted in the "Executive Order on Safe Secure and Trustworthy Development and Use of Artificial Intelligence" [White House 2023]).

ITL's Cybersecurity and Privacy for Genomic Data Processing project is studying all aspects of genomic security and privacy, encompassing current practices, risk assessment, and developing novel leading-edge solutions for storing and processing genomic data while minimizing risks of leakage and subversion. This work was directed by Congress and is partly in support of the Executive Order mentioned earlier.

### NCCoE Election Security Project

Voting is a keystone of our democracy. The nation depends on voting to be accessible to all voters, accurately tallied, and free from malicious interference. Voters must also have privacy in their ballots. Voting technology supports a wide variety of elections and ballot initiatives, from voting for town dogcatcher to voting for U.S. President, from local school board budgets to state constitutional amendments, and more. Furthermore, it is desirable to allow voting technologies to be produced by multiple vendors yet still meet all these conditions.

As a consequence of the Help America Vote Act (P.L. 107-252) in 2002, Voluntary Voting System Guidelines were developed. As threats from outside the country and within have been manifested in both the 2016 and 2020 national elections, the need for rigorous standards and testing has become even more critical. The Election Security project plays a key role in the development, evaluation, and update of the Voluntary Voting System Guidelines as well as related efforts, including guidance on accessible interfaces and physical security. As technology progresses and gaps are identified, ACD works with appropriate parties, including state Secretaries of State, the Department of Homeland Security, vendors, and the Election Assistance Commission to evolve practice and guidance.

### Cybersecurity and Privacy Small Business Outreach and Engagement Project

The Cybersecurity and Privacy Small Business Outreach and Engagement Project is a NIST initiative arising from the NIST Small Business Cybersecurity Act (P.L. 115-236) charged with

Copyright National Academy of Sciences. All rights reserved.

"disseminat[ing] clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks." The program is relatively new and currently relatively small.

Small businesses range from organizations with sole proprietorship to those with roughly 500 employees (the exact classification depends on the sector). Small businesses rarely have dedicated information technology (IT) staff, which means that they generally do not have the requisite skills to benefit directly from NIST cybersecurity guidance. This NIST outreach helps small and medium-size businesses use NIST standards and guidance to manage their risks. Outreach and engagement are discussed in detail in the section "Effectiveness of Dissemination Efforts" below.

### Privacy Engineering Program

ACD's Privacy Engineering Program is charged with "Support[ing] the development of trustworthy information systems by applying measurement science and system engineering principles to the creation of frameworks, risk models, guidance, tools, and standards that protect privacy and, by extension, civil liberties."[1] An additional strategic goal is to position ITL and NIST overall as a leader in privacy engineering to ensure that the institute is well placed to influence future privacy-related standards and practices. The work is authorized by the National Institute of Standards and Technology Act (15 U.S.C. 271).

One of the central deliverables of the Privacy Engineering Program is the NIST Privacy Framework (discussed below). The Privacy Framework is highly impactful, and some of this impact is clearly owing to the research and evangelism of the larger Privacy Engineering Program. The team has also directly and indirectly guided the development of international standards, for example, with the International Organization for Standardization (ISO) and International Electrotechnical Commission standards.

### Identity and Access Management Project

Digital identity schemes are proliferating rapidly in both the public and private sectors. Some states are issuing mobile driver's licenses. In addition, the OpenID Foundation and the FIDO Alliance, among others, have defined schemes that are being adopted in nongovernmental settings. One of the interesting initiatives is the creation of consortia to validate and study the use of mobile driver's licenses in government, health care, and financial settings. The use of mobile driver's licenses in these settings demands attention to usability and privacy and will probably require the development of additional protocols and standards; some of these points are elaborated on in the section "NCCoE Mobile Driver's License Project," earlier.

The ACD Identity Program is a multidisciplinary team with expertise ranging from mathematicians and cryptographers to policy specialists who address the challenges of developing and implementing digital identities. The team conducts research, develops standards, and guides and enables the adoption of digital identities. These areas will be studied by building testbeds for multiple end-to-end use cases.

### Cybersecurity and Privacy Frameworks

NIST's Cybersecurity Framework was first released in 2014 to help organizations understand, reduce, and communicate about cybersecurity risk. The Cybersecurity Framework is widely used within organizations to enable nontechnical management and technical cybersecurity practitioners to assess and manage cybersecurity risks.

[1] See NIST's "Privacy Engineering Program" website at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering, accessed September 26, 2024.

Copyright National Academy of Sciences. All rights reserved.

NIST's Privacy Framework was first released in 2020 to enable privacy engineering practices that help organizations protect the privacy of individuals. The Privacy Framework is structurally aligned with the Cybersecurity Framework and enables traceability for privacy protection activities to meet regulatory obligations. Organizations can use the two frameworks together to manage their cybersecurity and privacy risks. The ACD Privacy Engineering team is in the process of developing a Privacy Workforce Taxonomy consistent with the Privacy Framework to describe the tasks, knowledge, and skills needed within a workforce to manage privacy risk.

While the Privacy Framework is young, stakeholders have already indicated its value through their investments in crosswalks[2] to various laws, regulations, and standards (e.g., to the European Union's General Data Protection Regulation); translations of the Privacy Framework into other languages; and the development of profiles for different types of organizations.

### NICE Workforce Framework for Cybersecurity

The NICE Workforce Framework for Cybersecurity, commonly known as the NICE Framework, was first released in 2012 as a pivotal tool to enhance cybersecurity capabilities within the federal workforce. Originally established under the Comprehensive National Cybersecurity Initiative in 2008, the scope of NICE was expanded in 2009 to encompass the private-sector workforce.

NICE's mission is to energize, promote, and coordinate a robust community dedicated to advancing cybersecurity education, training, and workforce development. This mission has been pursued through collaboration with government, academia, and industry partners. NICE's strategic plan is intended to provoke a national dialogue and guide actions to address the critical shortage of skilled cybersecurity professionals. The NICE Community Coordinating Council and the NICE Interagency Coordinating Council facilitate public–private collaboration and federal coordination on policy initiatives and strategic directions in this domain. To accomplish its mission, NICE

- Hosts an annual conference and expo
- Hosts an annual K–12 Cybersecurity Education Conference
- Hosts an annual Cybersecurity Career Week
- Conducts webinars
- Hosts a Federal Cybersecurity Workforce Summit and Webinar Series
- Manages Federal Information Security Educators, an organization that helps federal agencies strengthen their workers' cybersecurity awareness, and runs training programs to that end

### NIST Cybersecurity for the Internet of Things Program

The Cybersecurity for the Internet of Things (IoT) program supports the development and implementation of standards, guidelines, and tools aimed at enhancing the cybersecurity of IoT systems, products, and environments. This program collaborates with stakeholders across government, industry, academia, international bodies, and consumers to build trust and foster global innovation. NIST IR 8316, *Internet of Things (IoT) Component Capability Model for Research Testbed* (NIST 2020a), elaborates that IoT systems consist of networked components interacting with physical entities through sensors or actuators, distinguishing them from conventional IT systems, which do not interact directly with the physical world. NIST has further defined an IoT product in NIST IR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products* (NIST 2022b), as comprising one or more IoT devices and related

[2] From NIST's Privacy Framework website, "These crosswalks are intended to help organizations to understand which Privacy Framework Functions, Categories, and Subcategories may be most relevant to addressing the provisions of the source document. Organizations should not assume implementation of these Privacy Framework activities or outcomes means that they have met the provisions of the source document. There may be other activities that organizations need to undertake" (NIST 2024a).

Copyright National Academy of Sciences. All rights reserved.

components such as networking hardware, companion application software, and backend services. These products can form complex IoT systems that serve consumer needs. The publication is intended to help manufacturers produce more secure IoT products and assist organizations in securing those products.

The IoT program encompasses a broad spectrum of activities designed to ensure comprehensive and inclusive input. These activities include leveraging existing NIST guidance, conducting landscape reviews, considering publicly available information on past events, and consulting informally with academic, civil society, and industry experts. Public interactions are facilitated through numerous in-person and virtual workshops, garnering significant participation, and extensive engagement with almost 2,000 public comments across draft and final publications. ACD IoT program staff members also actively participate in standards development, bilateral and multilateral governmental discussions, and present findings at domestic and international conferences. Key stakeholders actively involved in NIST's IoT program include the following:

- U.S. government agencies such as the Food and Drug Administration, Department of Energy, and Cybersecurity and Infrastructure Security Agency
- Various NIST organizations
- International government agencies such as the EU Commission and the European Union Agency for Cybersecurity (i.e., ENISA)
- Standards development organizations such as ISO and the International Electrotechnical Commission
- Academic institutions such as the Massachusetts Institute of Technology and Carnegie Mellon University
- Civil society organizations such as the Center for Democracy and Technology
- Industry groups such as the U.S. Chamber of Commerce and the Information Technology Institute

## Accomplishments

### *Small Business Cybersecurity and Privacy Outreach Program*

To date, this program has focused on coordinating NIST's cybersecurity efforts with small and medium-size business-related programs and relationships across the federal government, building relationships with partners, and educating small and medium-size businesses about NIST's cybersecurity resources. The community-building and education program creates tailored web resources—offering guidance by sector and topic—and webinars. Web metrics—the number of page views, downloads, and webinar attendees—indicate that the program has started well.

### *National Cybersecurity Center of Excellence*

NCCoE "How-To Guides" document the process of installing and configuring the commercial products in one or more NCCoE project implementations. To ensure that the setup process for the exemplar cybersecurity solutions is replicable, the guides provide detailed configuration instructions, including screenshots of setup windows, the options selected in pull-down menus, and the sequence of button clicks.

### *Migration to Post-Quantum Cryptography Project*

This program appears to be managed well and is making good progress. Draft documents providing guidance were published at the end of 2023. Laboratory demonstrations of performance and interoperability tools were performed this year. The effort has also resulted in the formation of a large, active, and appropriate working group of more than 1,600 members from both industry and government.

Copyright National Academy of Sciences. All rights reserved.

Publications and presentations appear to be attracting community engagement. The effort to date is commendable and the topic is potentially critical. The plans for future steps appear reasonable, and it is important that appropriate resources be applied to this effort maintain and add appropriate resources to maintain progress.

*5G Security Standards and Applied Research and the Zero Trust Laboratory Project*

The ACD 5G Cybersecurity Project has produced a range of publications and has built a 5G testbed to guide the management of 5G cybersecurity risks. Notably, volumes of NIST SP 1800-33 (draft), *5G Cybersecurity NIST SP 1800-33 Practice Guide Preliminary Draft* (NIST 2021a), and various cybersecurity white papers offer detailed guidance. Additionally, ACD provides recorded demonstrations and informational sessions to further educate stakeholders on 5G security best practices.

*NIST Cybersecurity Framework Profiles Project*

This project has put out several Community Profiles. A few examples of Community Profiles that illustrate their application across different sectors and use cases are

- Cybersecurity Framework 1.0 Community Profiles: Manufacturing, Maritime Specific, Communications Sector, among others.
- Cybersecurity Framework 1.1 Community Profiles: Manufacturing, Election Infrastructure, Ransomware Risk Management, Liquefied Natural Gas, Hybrid Satellite Networks, Genomic Data, Electric Vehicle Charging, Smart Grid, and more.
- Cybersecurity Framework 2.0 Community Profiles: Incident Response Recommendations, Cyber Risk Institute Profile for the Financial Sector.

As of this writing, the guide is currently under review, with public comments being analyzed. Additionally, the panel noted that they need to continuously develop additional community profiles, engage new and existing communities, expand content in the Framework Resource Center, and refine the community profiles template.

*Cybersecurity and Privacy for Genomic Data Processing Project*

The starting point for this work is understanding and quantifying risk. Many of the risks are common to other data sets, but there are enough unique challenges to warrant the development of sector-specific evaluation metrics. ACD approached this by developing testbeds and domain-specific cybersecurity frameworks and profiles. Risk quantification is guided by NIST IR 8477, *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings* (NIST 2024b). This report defines security objectives (e.g., “Preserve Privacy of Donors”) and details the security principles and best practices that can contribute to the security mission. ACD collaborated with health and genomics experts in this work. The relevant experts in both cybersecurity and genomics contributed beneficially, and community feedback on the value of this work has been positive.

*Election Security Project*

Voting and vote counting have become highly politicized topics. The NCCoE efforts in this area have kept focused on verifiable and understandable technical guidance. Wider understanding and acceptance of this guidance, and testing real systems against it, is one way to quiet some of the suspicions and disagreements in this arena.

ITL has played a key role in the development, evaluation, and update of guidelines to secure elections, as well as in related efforts including guidance on accessible interfaces and physical security. As technology has progressed and gaps have been identified, ACD has worked with the appropriate parties, including state Secretaries of State, the Department of Homeland Security, technology vendors, and the Election Assistance Commission to continually develop practice and guidance in response to new threats and challenges. In particular, ACD has supported the development of the Voluntary Voting System Guideline 2.0 and the promotion of fundamental ideas such as software independence and risk-limiting audits. Its Voting Technology Series of guidance documents is particularly valuable to the community (NIST 2024c). ACD is to be commended for its careful and highly valuable work in this topic area. It is vitally important that this be an ongoing effort, maintained at a level appropriate for the needs involved.

### *Privacy Engineering Program*

One of the central deliverables of the Privacy Engineering Program is the NIST Privacy Framework, which is described in more detail above. In addition to this foundational work, the Privacy Engineering team has developed a collection of privacy engineering–related tools and a collaboration space. These resources allow NIST and other expert practitioners to study topics such as disassociability (using differential privacy and other techniques) and assessing privacy risks. The team has also sponsored competitions to advance the understanding and adoption of privacy-enhancing technologies. One recent focus is maintaining privacy in federated machine learning. Also of note is the Privacy Risk Assessment Methodology, which drastically reduces the time that it takes to discover and quantify a privacy risk. The Privacy Engineering Program has advanced and promoted the state of the art in privacy in differential privacy (adding statistical noise) and federated learning (learning without actually sharing data).

### *Identity Program*

A foundational component of the Identity Program is the NIST 800-63 family of guidelines that address the management and use of digital identities. These special publications are directed toward federal agencies' use of digital identities, but they are applicable to nongovernmental use as well.

These special publications are highly influential in how digital identities are being managed and adopted. Elsewhere in this report, it is argued that simple engagement counts are a poor indicator of NIST's societal impact, but here it bears noting that there were approximately 3,800 comments during the public comment period for the fourth revision, with 70 percent coming from the private sector—a clear indicator of the importance of this work.

### *Identity and Access Management Project*

An important aspect of this work is coordinating U.S. efforts with the EU approach to digital identity codified in eIDAS regulation.[3] This mapping effort is particularly important because the European Union is pursuing a mandatory regulatory approach, while the United States mainly provides noncompulsory guidance. The draft *EU–U.S. TTC WG-1 Digital Identity Mapping Exercise Report* (NIST 2023) will help ensure that the ecosystems are aligned and hopefully interoperable for some scenarios, something that is important for U.S. industries and technologies to compete globally.

ACD's identity program is having an outsized impact, both within the federal government (e.g., the Social Security Administration, Internal Revenue Service, and Department of Health and Human Services), by the states (e.g., mobile driver's licenses), and in the private sector (perhaps a billion users protected by phishing-resistant authenticators, according to Google and the FIDO Alliance).

### *NICE Workforce Framework for Cybersecurity*

Internationally recognized, the NICE Framework has been adopted and translated by organizations worldwide, including those in the United Kingdom, Canada, and Australia, demonstrating

[3] See the European Commission's website "eIDAS Regulation" at https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation, accessed August 21, 2024.

Copyright National Academy of Sciences. All rights reserved.

its global influence. NICE is currently exploring the development of industry-specific profiles to tailor the framework to various sectors, enhancing its applicability and flexibility. Also, the NICE Framework Resource Center offers tools, guides, and resources to support the implementation and use of the framework, reinforcing its role as a critical tool for maintaining national cybersecurity. Through these efforts, NICE continues to lead in promoting cybersecurity education and workforce development, coordinating NIST cross-functional teams, interagency coordination, stakeholder engagement, and international harmonization. There have been approximately 1,644 downloads of NICE Framework v1.0.0 and more than 20,000 views by nearly 13,000 users of the NICE Framework Resource Center landing page since March 2024. In addition, there has been a 40 percent growth in members of the NICE Framework Users Group in FY 2024.

*NIST Cybersecurity for IoT Program*

Notable accomplishments of the NIST Cybersecurity for IoT program include receiving the World Innovation, Technology, and Services Alliance Chairman's Award in 2023. NIST's IoT definition from NIST IR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* (NIST 2020a), was cited in the IoT Cybersecurity Improvement Act (P.L. 116-207). Since 2017, this program's publication suite has seen more than 275,000 downloads with several publications translated into Spanish and Portuguese.

Publications such as NIST SP 800-213/-213A, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (NIST 2021b), form the basis for the Office of Management and Budget's Federal Information Security Management Act guidance on IoT, and the NIST Consumer Profile underpins the Federal Communications Commission U.S. Cyber Trust Mark criteria. NIST's IoT cybersecurity research has been recognized as an inspiration for the EU Cyber Resilience Act critical criteria and recommended by the Federal Trade Commission for IoT product manufacturers. Additionally, California amended its IoT Security Law to provide a safe harbor for connected device manufacturers complying with NIST criteria. International standards ISO 27402 and American National Standards Institute-2088 were based on NIST IR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* (NIST 2022a), and American National Standards Institute/Consumer Technology Association 2119, "Framework for Evaluation of a Cybersecurity Scheme," currently in development, is based on NIST IR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products* (NIST 2022b).

Overall, the NIST Cybersecurity for IoT Program plays a crucial role in improving the cybersecurity of IoT systems and devices. Its guidance publications, engagement with stakeholders, and impact on legislation and industry practices demonstrate its effectiveness in addressing the unique challenges of IoT cybersecurity. By fostering trust and enabling innovation, the program contributes to a more secure and resilient IoT ecosystem.

## Opportunities and Challenges

There has been recent revolutionary progress in foundational artificial intelligence (AI) and its application. It is expected that AI will impact most aspects of life and commerce in the next few years. However, the impact of AI on the field of computer security is currently unclear. AI can be used by both attackers and defenders, and new AI-powered products and services will introduce new risks that are currently not understood. There are also increased privacy concerns related to the data used to train AI systems. It is vitally important that the responsible use of AI be explored and addressed. At the time of writing, the panel does not have specific recommendations for new AI-focused projects or new AI-related workstreams on existing projects but believe that developing staffing, equipment, and expertise in AI will be critical for ACD to be effective in the next decade.

Copyright National Academy of Sciences. All rights reserved.

Cutting-edge research, model training, and inference all demand a significant investment in hardware, data and software, operations (e.g., power), and staff. Developing these capabilities will be expensive, and talent will be recruited only if the facilities are of a high caliber.

> **Recommendation 3-1: Existing and new Applied Cybersecurity Division projects should include the study of the security, privacy, and responsible uses of artificial intelligence (AI), including the security and privacy characteristics of AI systems.**

### *Small Business Cybersecurity and Privacy Outreach Program*

It is particularly challenging for small non-IT-sector businesses—approximately 80 percent of U.S. small businesses are single-proprietorships—to apply ACD guidance. Much of the available guidance designed for small businesses—provided by organizations including the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, the Small Business Administration (SBA), and the Federal Trade Commission—assumes organizational roles that do not exist in single proprietorships or partnerships. It would be wasteful for ACD to expend its limited resources to develop materials that are somewhat duplicative of existing federal resources and do little to help the many tiny businesses that are underprotected from cyberattacks. Also, the gap between the estimated number of small businesses—approximately 30 million—and the size of the current community—approximately 1,000 attendees for a webinar—is considerable.

In contrast, by developing new, streamlined guidance specifically tailored for businesses that employ at most five individuals, ACD could assist the large majority of the small business community that is currently underserved by existing information sources. For example, ACD could partner with the SBA to develop and host training videos, checklists, and other materials that target this community. The SBA has regional centers that host events, which could include cybersecurity outreach and education. ACD’s educational reach could be extended by focusing on training the SBA trainers in SBA regional communities.

> **Recommendation 3-2: The Applied Cybersecurity Division (ACD) should focus on the development of new, specialized cybersecurity guidance for single proprietor or partnership businesses with only a few employees. It should partner with the Small Business Association to develop training materials such as videos and checklists and support regional outreach to enable ACD to have a broader impact within the limited resources available to the program.**

### *National Cybersecurity Center of Excellence*

Whenever possible, it is advisable that NCCoE’s individual projects use Configuration as Code tools—such as Ansible, Puppet, Chef, and SaltStack—or Infrastructure as Code tools such as Terraform to record project technology configurations and setup steps. Using such tools will allow the creation of configuration manifests that can succinctly capture the technical steps used to deploy and configure technologies and enable automated, replicable deployment of specific cybersecurity solutions. Such manifests are also amenable to analysis by automated configuration assessment tools, which can highlight configuration conflicts or security issues. Publication of configuration manifests to a code repository such as GitHub could enable NCCoE teams to more concisely express technical deployment details and enable a clearer understanding and assessment of the applicability and improved replicability of NCCoE engineering work.

### *5G Security Standards and Applied Research and the Zero Trust Laboratory*

Despite its strengths, this effort can be improved by enhancing scalability and ensuring interoperability among different vendors’ equipment and security solutions instead of focusing on a single vendor stack.

Copyright National Academy of Sciences. All rights reserved.

*Zero Trust Project*

To further improve the Zero Trust project, several enhancements can be considered. First, enhancing interoperability with a wider range of legacy systems and emerging technologies than is currently the case can facilitate smoother transitions. Second, expanding use cases and scenarios in practice guides can offer more tailored solutions, addressing unique challenges in various sectors. Third, incorporating more automation into zero-trust implementations can help manage security policies and responses more efficiently. Last, developing comprehensive training programs for IT staff and end users seeking to deploy zero-trust solutions can ensure better implementation and adherence to security protocols such as closer collaborations with parallel initiatives such as NICE.

*NCCoE Mobile Driver's License*

It would be useful for the project team to consider further expanding the testbed and use cases to address trade credentials. International import and export currently rely on paper-based credentials (or digital representations from scanned paper) that document the characteristics and provenance of products and their components for manufacturers, shippers, customers, and government regulators. Verifiable digital credentials for trade have the potential to both improve security and streamline international import and export processes. Security requirements for trade credentials are likely to differ from those for digital identities. Stringent technical privacy requirements for digital identities, especially to prevent the tracking of individuals, are almost inverted for product provenance credentials: tracking the provenance of product components and aggregation of production certifications (e.g., environmental and anti-forced labor) are necessary. The set of potential industry, government agencies, and other institutional collaborators for digital identity projects such as the current Mobile Driver's License project and future projects involving other verifiable identity credentials is likely to differ greatly from those that will participate in projects involving trade credentials.

*NIST Cybersecurity Framework Profiles*

Considerable effort has gone into making the Cybersecurity Framework Profiles. In theory, these profiles should see widespread use. However, no plan to evaluate the adoption and effectiveness of these profiles was presented. Such a plan, or plans, is important to understand how effective the division is in helping users implement cybersecurity approaches and in guiding future efforts along these lines. The standard period for public comment will result in self-selected respondents who may not adequately represent the target demographic. An active effort will yield better results. ITL's Statistical Engineering Division might be able to help with this.

> **Recommendation 3-3: The Applied Cybersecurity Division should conduct a study of the target audiences for its Cybersecurity Framework Profiles to determine if they are being used to full effect, and to determine if their content and format are appropriate for the intended audiences. The Statistical Engineering Division should be consulted on this. Future profiles and the allocation of resources to support their development should be informed by this study.**

*Cybersecurity and Privacy for Genomic Data Processing*

One of the particularly interesting challenges in genomic data sets is that competitive threats in combination with ethical and regulatory considerations lead to data sets that are typically fragmented across different companies, research laboratories, and hospitals. There is a widespread belief that aggregating these data sets for analysis will lead to deeper insights, but the risks of data theft or disclosure make this undesirable. Privacy-enhancing technologies offer mechanisms that allow computation across different data sets with limited and controlled disclosure of the underlying data itself. ACD is exploring the use of privacy-preserving federated machine learning to address this challenge. This approach certainly has merit. Alternative approaches, perhaps based on confidential computing, could also be

Copyright National Academy of Sciences. All rights reserved.

explored to understand the strengths and weaknesses of each. ACD is to be commended for this important work and the panel fully supports ACD's assessment that the techniques being developed in this area are applicable to many other scenarios outside genomics and health care.

### *Identity and Access Management*

ACD could invest more into the study of the robustness of various implementations of digital identities, particularly how systemic risks can be mitigated, and of identity ecosystems that can be rebuilt in the case of a large and effective cyberattack. As digital identities are used for more scenarios, the attractiveness of the digital identity ecosystems as cyber-targets will grow. As identity is the basis for almost all other services, it is particularly critical that these ecosystems are resilient and recoverable.

> **Recommendation 3-4: The Applied Cybersecurity Division should supplement its work on digital identities with a study of the implications and remediation of a large-scale cyberattack on modern identity systems, such as what might arise from vulnerabilities in widely used desktop or mobile operating systems.**

### *Privacy Framework*

The panel encourages the Privacy Framework team to emphasize investment-based impact metrics for different stakeholder communities. For example, a law firm with a large practice in digital assets and data management invested significant effort to develop a crosswalk between the Privacy Framework and the California Consumer Privacy Act of 2018. Such stakeholder investment is a strong indicator of the value of the Privacy Framework to the legal community.

## ASSESSMENT OF SCIENTIFIC EXPERTISE

ACD reports FY 2023 staffing levels of 184 associates, 44 scientists, and 2 support staff.[4] Figure 3-1 shows the ACD staff levels from FY 2015 through FY 2024. It can be seen that permanent ACD staff levels have fluctuated but appear to have been fairly level since FY 2020. The number of associates, however, has shown significant change, with a dramatic increase in FY 2016, rising to a maximum in FY 2022, and decreasing after that. While ACD reports 184 associates in FY 2023, it can be seen that there are significantly fewer associates in FY 2024.

ACD did not provide detailed information on staff honors and awards. They reported that their staff have won nine internal and external awards. However, awards and honors are not the only measures of quality. Based on interactions with the staff over the course of the meeting, it is clear that the overall expertise of the ACD staff is excellent.

Furthermore, ACD staffs its projects with scientific experts from across ITL and NIST more broadly and collaborates with other national and international government agencies, industry, and academic institutions. The resulting project teams create a world-class workforce of internal and external subject-matter experts to advance standards and guidelines. The depth and breadth of the researchers accelerate impactful outcomes for the broader cybersecurity community.

[4] Associates are not NIST employees. They are outside researchers, both foreign and domestic, who collaborate with NIST researchers.

Copyright National Academy of Sciences. All rights reserved.

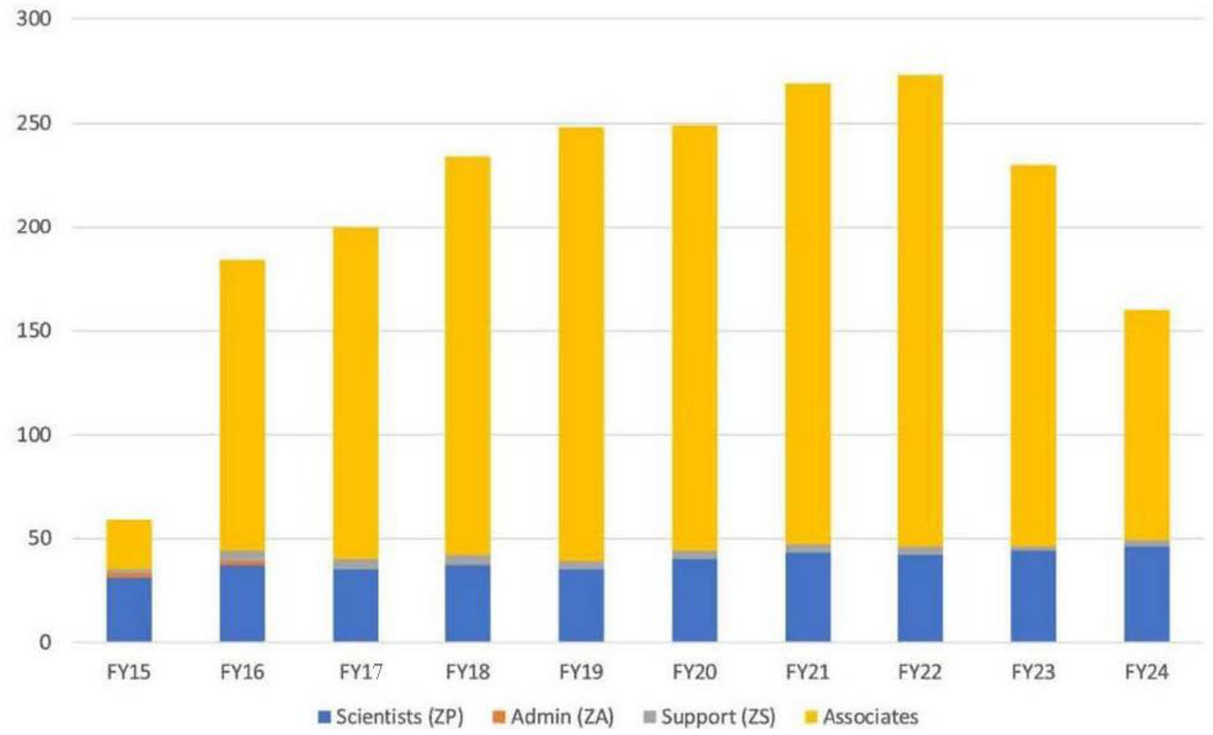


**FIGURE 3-1** Applied Cybersecurity Division staffing from fiscal year (FY) 2015 through FY 2024.
SOURCE: Courtesy of NIST Information Technology Laboratory.

## BUDGET, FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

ACD's FY 2024 budget is $62 million. Figure 3-2 shows ACD budget levels and trends from FY 2016 through FY 2024. The budget has three major components: congressional scientific and technical research services (STRS) appropriations, internal funding competitions such as the Innovations in Measurement Science internal grant competitions, and work done for other federal agencies.

ACD is an excellent steward of funds: it engages creative and effective strategies to staff critical projects. It is notable that while the ITL budget has increased by approximately 20 percent between FY 2016 and FY 2024 (staff growth has not matched budget growth because labor costs have grown), it has not kept pace with the growth of the IT sector. By some measures, IT sector revenues have doubled since 2016.[5] Other business sectors are increasingly dependent on advances in IT. As IT powers more and more businesses, sectors, and governmental functions, the attractiveness of IT systems as cybertargets grows commensurately. ITL, and NIST broadly, is foundational to how the nation secures its infrastructure, and the panel believes that greater investment in ITL would lead to increased growth and stability of the IT sector and the businesses it powers, reduced cybercrime, and decreased risk of catastrophic black-swan events.

In the course of the meeting, the panel toured some of the laboratories and other facilities in NCCoE and on the Gaithersburg, Maryland, campus. Overall, they are adequate to support the needs of ACD and ITL more broadly.

[5] See Statista's "IT Services—United States" website at https://www.statista.com/outlook/tmo/it-services/united-states, accessed August 21, 2024.

Copyright National Academy of Sciences. All rights reserved.

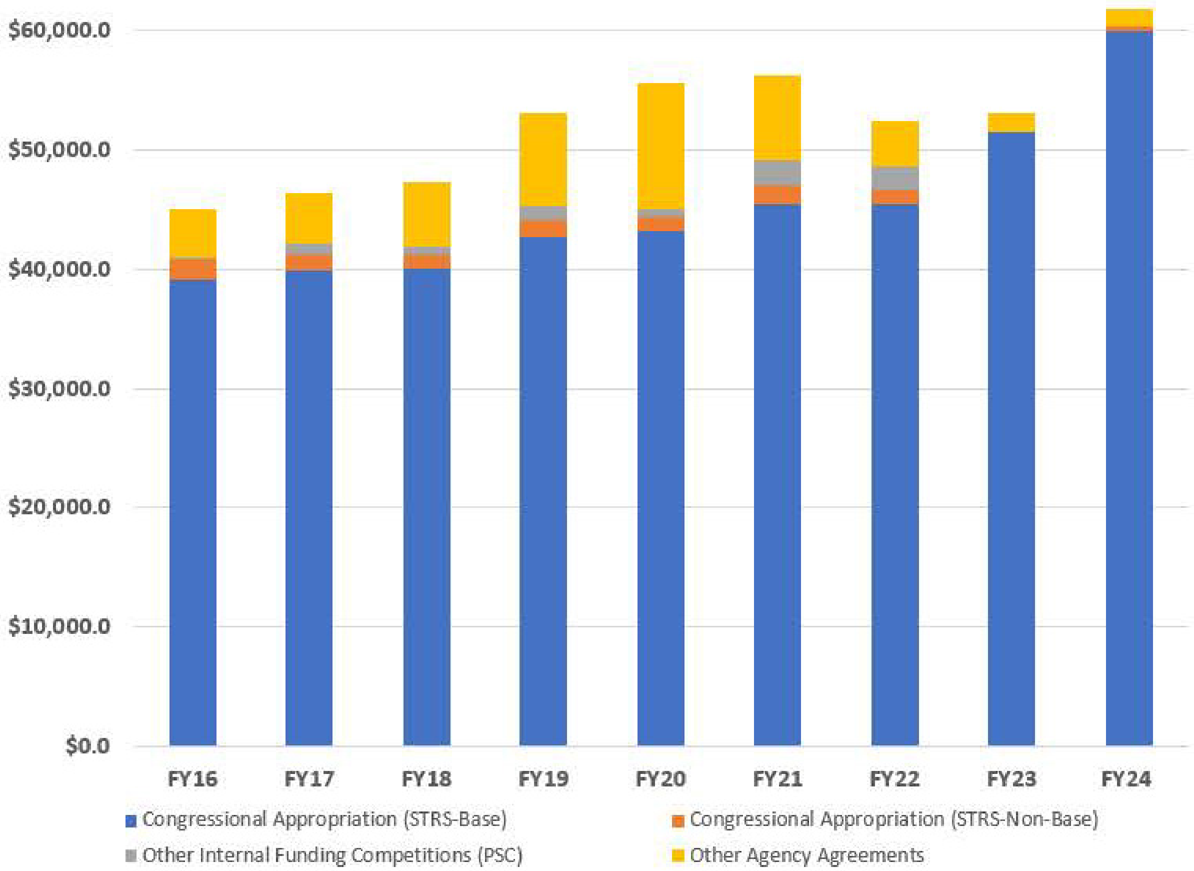


**FIGURE 3-2** Applied Cybersecurity Division budgets from fiscal year (FY) 2016 through FY 2024.
NOTE: PSC, Public Safety Communications; STRS, scientific and technical research services.
SOURCE: Courtesy of NIST Information Technology Laboratory.

The risk of losing key staff and expertise, particularly because of the laboratory's current demographics, is concerning. A large proportion of ACD staff is eligible for retirement within the next 10 years. Specifically,

- 26.1 percent are eligible to retire now.
- 6.5 percent will be eligible in 3 years.
- 2.2 percent will be eligible in 5 years.
- 8.7 percent will be eligible in 10 years.
- 56.5 percent will be eligible beyond 10 years.

Among the nation's senior IT and computer security engineers, there is a strong appetite for engaging in unpaid community service to "make a difference." The volunteers on this panel are a good example of this. This includes senior cybersecurity engineers, not only researchers. The panel advises that ACD explore creative, and hopefully inexpensive, approaches to tapping into this underused resource. This might include developing visiting engineer programs or collaborations in addition to NIST's existing visiting researcher programs.

Copyright National Academy of Sciences. All rights reserved.

**Recommendation 3-5: The Applied Cybersecurity Division (ACD) should explore innovative approaches to staff augmentation and retention. ACD should also develop programs to engage senior volunteer cybersecurity research and engineering talent to serve the nation through its programs and activities.**

## EFFECTIVENESS OF DISSEMINATION EFFORTS

A key part of ACD's mission is to ensure that NIST standards and guidance are practical and effective. ACD attributes part of its effectiveness to the fact its staff "listen, lead, and are trusted." This aphorism captures an important feedback loop: for ACD to be effective, it must provide high-quality and useful standards and guidance. This requires experts—from both within and outside NIST—to volunteer their time, which they will do only if they believe that they can influence NIST's work product and that the results are valuable and important. ACD staff have built healthy and active communities of users and experts for most of the projects assessed in this report. The open and collaborative approach taken by the staff of ACD has led to these successes.

ACD staff also noted at the meeting that "We work quietly behind the scenes, ensuring the things you rely on daily are safe, reliable, and compatible. Think of us as the invisible force powering everything from your smartphone to the bridges you cross." The panel supports this assessment but believes that more visibility, and perhaps more importantly, better quantification of the impact on U.S. competitiveness, would result in resources commensurate with the size of the existing challenges and opportunities.

The panelists from the private sector stress how important and influential NIST standards and guidance are to their businesses. Adherence to NIST standards reduces risks, reduces costs, and increases competitiveness far beyond the measurable impacts that NIST cited. NIST is a crown jewel of our national laboratories for IT.

ACD provided the following dissemination metrics for FY 2021 through FY 2023:

- 624,000 total ACD publication downloads
- 5.7 million visits to the Cybersecurity Framework website, the most-visited site in NIST
- Approximately 75,000 followers on the @NISTcyber X account, nearly double those in FY 2021
- 54 publications, including special publications (in the 800 and 1800 series among others), interagency reports, internal reports, and white papers
    - 25 in FY 2021
    - 19 in FY 2022
    - 10 in FY 2023
- 45 blogs, promoted via GovDelivery and X, with approximately 95,000 views
- More than 15,000 registrants for events, workshops, and conferences

ACD's efforts to engage stakeholders and monitor the impact of individual ACD projects are impressive.

ACD's methods for continuous and periodic feedback, broad stakeholder engagement, and comprehensive workshops promote successful collaboration of scientific experts. ACD actively hosts webinars and meetings to update the ecosystem on project status. The team also presents at and participates in industry conferences and working groups to foster collaboration. Furthermore, ACD engages with various international governments to discuss and develop strategies for managing cybersecurity risks. However, the impact metrics are inconsistent and somewhat lacking. The size of a community as measured by webinar participation or download counts is interesting but is not a fair or complete measure of the actual value of ACD's outreach and dissemination. In general, ACD projects are

Copyright National Academy of Sciences. All rights reserved.

undervalued and their impact underappreciated. ACD needs to develop improved metrics for individual projects that focus on the quality and magnitude of their impact.

Note that all who participate in communities of practice are self-selected. To truly assess the impact on the intended communities, ACD needs to randomly select intended stakeholders from whom to solicit input. It is understood that there are constraints on ACD's ability to solicit information about stakeholder use and impact, such as Office of Management and Budget mandates regarding conducting surveys, but the panel encourage the development of metrics that go beyond counting the number of downloads.

One source for ideas might be the open-source community and how they measure the impact and use of an open-source project. For instance, it might be interesting and useful to track the quantity and frequency of external contributions to ACD documents and the number of issues reported by adopters and implementers. More ideas can be found in the section "What to Track" on the Linux Foundation website, Measuring Your Open Source Program's Success.[6]

For NCCoE projects, one metric of industry value might be the percentage of collaborating companies that are repeat participants, participating in two or more NCCoE projects. Such a measure might apply differently to small, narrowly focused start-ups than to large, established technology companies.

> **Recommendation 3-6: The Applied Cybersecurity Division should develop impact metrics for individual projects and apply them uniformly. Metrics should include economic benefits for adopters and quantification of risk reduction, where possible. Useful ideas may be found, for example, through the open-source community and the Linux Foundation.**

## PLANNING

As noted earlier, the panel has some concerns that adequate resources be provided to ACD for its important work. New projects are being mandated by legislation and executive orders, and AI, cloud computing, complex supply chains, and other advancements are profoundly changing the practice of and science of computer security.

ACD also faces the potential for significant retirements leading to questions about there being adequate experience to support ACD's work in the future. The panel is concerned that at the current level of staffing and the rate at which new projects are mandated, there is a risk of staff and expertise being spread too thin, leading to reduced value and impact from ACD's work.

> **Recommendation 3-7: The Applied Cybersecurity Division (ACD) should develop and share a strategic vision for how projects are selected and managed in ACD to balance the demands on the division with the available resources and prevent the loss of value and impact from being overstretched.**

## REFERENCES

NIST (National Institute of Standards and Technology). 2020a. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. IR 8259. May. https://csrc.nist.gov/pubs/ir/8259/final.

NIST. 2020b. *Internet of Things (IoT) Component Capability Model for Research Testbed*. IR 8316. September. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8316.pdf.

[6] See the Linux Foundation's Open Source Guide "Measuring Your Open Source Program's Success," at https://www.linuxfoundation.org/resources/open-source-guides/measuring-your-open-source-program-success, accessed August 21, 2024.

Copyright National Academy of Sciences. All rights reserved.

NIST. 2021a. *5G Cybersecurity NIST SP 1800-33 Practice Guide Preliminary Draft*. February 1. https://www.nccoe.nist.gov/publications/practice-guide/5g-cybersecurity-nist-sp-1800-33-practice-guide-preliminary-draft.

NIST. 2021b. *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. SP 800-213. November. https://csrc.nist.gov/pubs/sp/800/213/final.

NIST. 2022a. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. IR 8259. May. https://csrc.nist.gov/pubs/ir/8259/final.

NIST. 2022b. *Profile of the IoT Core Baseline for Consumer IoT Products*. IR 8425. September. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf.

NIST. 2023. *EU-US TTC WG-1 Digital Identity Mapping Exercise Report*. Updated December 22. https://www.nist.gov/identity-access-management/eu-us-ttc-wg-1-digital-identity-mapping-exercise-report.

NIST. 2024a. "Crosswalks." Updated May 8. https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks.

NIST. 2024b. *Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings*. IR 8477. February. https://csrc.nist.gov/pubs/ir/8477/final.

NIST. 2024c. "NIST Technical Series Publication List: VTS." Updated March 13. https://pages.nist.gov/NIST-Tech-Pubs/VTS.html.

Stine, K., and R. Petersen. 2024. "2024 NASEM Review: Applied Cybersecurity Division." Presentation to the panel. National Cybersecurity Center of Excellence. June 4.

White House. 2023. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." October 30. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

Copyright National Academy of Sciences. All rights reserved.

# 4
# Applied and Computational Mathematics Division

The Applied and Computational Mathematics Division (ACMD) develops mathematical and computational methods and tools that enable world-class measurement science. It collaborates with other divisions of the Information Technology Laboratory (ITL) and other laboratories across the National Institute of Standards and Technology (NIST), as well as other federal agencies to apply sophisticated mathematics, computational expertise, and tools to measurement and standards problems, with the goal of advancing trust in measurement and technology in service to the nation. It shares its results, reference data, tools, and standards with the scientific community.

Critical and emerging technologies in which the division has played a substantial part include the following:

- Advanced computing, including advanced modeling and simulation, and data processing and analysis
- Advanced engineering materials, including materials by design
- Artificial intelligence (AI), including machine learning, and AI assurance and assessment
- Biotechnologies, including biometrology, computational biology, and predictive modeling
- Semiconductors and microelectronics, including novel materials and specialized hardware
- Quantum information, including quantum computing, quantum sensing, and quantum communications
- Human–machine interfaces, including virtual reality and augmented reality

Not every project presented to the panel is discussed in the report. Only those projects about which the panel had comments are discussed.

## ASSESSMENT OF TECHNICAL PROGRAMS

Overall, ACMD is both broad and deep, including state-of-the-art expertise and infrastructure for applied and computational mathematics, visualization, quantum computing and communications, and AI modeling. Their work is motivated by the needs of the nation, including international competitiveness and national security.

### Accomplishments

A portfolio of projects was presented to the panel that reflected a broad spectrum of research capabilities within the mathematical modeling, analysis, and knowledge management spaces, as well as quantum information. This portfolio encompasses different types of fundamental mathematical modeling contributions (e.g. simulation, probability, machine learning, signal processing, and quantum algorithms), supporting resources and methodologies (e.g., knowledge management, visualization, and Internet of Things [IoT] devices), experimentation (with an emphasis on quantum computing and networks), and

Copyright National Academy of Sciences. All rights reserved.

application areas (e.g., medicine, energy, physics, and quantum computing). Several key portfolio areas and major contributions are highlighted below.

Classifying and identifying seized drugs with mass spectral library searching has demonstrated end-to-end contributions ranging from the development and maintenance of compound databases and analysis software to the highly impactful application of early detection of Fentanyl and other illegal drugs.

The NIST Digital Library of Mathematical Functions and Mathematical Knowledge Management is a large-scale library resource that has been systematically expanded and maintained for decades. This resource is widely known and used in the mathematics and scientific communities and has been cited more than 10,000 times in the past 14 years.

The Object Oriented MicroMagnetic Framework (OOMMF) forms the bedrock of many computational efforts in micromagnetics by providing a collection of portable and extensible public-domain programs. This effort has successfully built and sustained a community of users over the past 2 decades, with more than 3,700 citations since its inception. The commitment to long-term sustainability and quality control as illustrated by the OOMMF effort is a distinctive characteristic of NIST.

The Analysis of Separable Shape Ensembles project has demonstrated a deep and principled application of mathematical modeling for an underresearched but high-impact problem: shape analysis. While grounded in a concrete modeling problem (the design of wind turbines and airfoil shapes in general), the project is developing a principled representation of shapes, which can lead to a rich follow-up research program at the interface between shape analysis, deep mathematical modeling, and machine learning.

The Analysis of Diagnostics: Prevalence, Uncertainty Quantification, and Classification Theory research program has demonstrated the ability to attack high-complexity problems in an end-to-end fashion ranging from devices to highly informed mathematical models, and to package them within a high-impact health application area (i.e., cytometry). This project resulted in the creation of Lumos NanoLabs, a company that plans to commercialize the NIST microfluidic flowmeter.

The Computational Modeling of a Wearable System to Monitor Pulmonary Edema project models wearable networked IoT devices with supporting signal analysis and has been demonstrated within a sophisticated 3D visualization model. The group has long-term international leadership in wearable networks and IoT for health, as demonstrated by their development of high-fidelity computational models of the human lungs essential for benchmarking wearable devices, regular organization of special sessions at international conferences, and significant contributions to international standards in this area, such as Institute of Electrical and Electronics Engineers (IEEE) 802.15.6, IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks.

Another set of portfolio projects centered around quantum computing and quantum networks. The Joint Center for Quantum Information and Computer Science—known as QuICS—is a collaborative center co-hosted by NIST and the University of Maryland (UMD). The research group articulated a highly successful partnership where NIST resources are augmented and complemented by UMD. This strategic partnership has demonstrated international leadership in the areas of quantum algorithms and quantum cryptography, as evidenced by their steady publications in top-tier journals, their lead in the creation of the Error Correction Zoo (an online catalog of more than 900 classical and quantum error correction codes), and more significantly, their contributions to the federal information standards for post-quantum cryptography: Federal Information Processing Standards 203, 204, and 205. This partnership allows NIST to access academic expertise, collaborative grants, and human resources as well as to benefit the UMD community and should be considered a gold standard for similar types of collaborations.

ITL researchers have world-leading expertise in quantum cryptography. In collaboration with the Computer Security Division and other NIST laboratories, ITL has made significant contributions to a Post-Quantum Cryptography Standardization program that was announced in 2016 as a competition by NIST to update the standards to include post-quantum cryptography. Final versions of the first three Post Quantum Crypto Standards were released by NIST on August 13, 2024.

One example of recent high-impact work on quantum algorithms is the understanding of the power of forgetting for quantum algorithms. Researchers at ITL and QuICS proved that, with reasonable

Copyright National Academy of Sciences. All rights reserved.

assumptions, to maintain an exponential speedup over any classical algorithms on a particular problem of finding an exit in a maze, the quantum walk algorithm must forget the path to get to the exit. This work sheds new light on fundamental understanding of what quantum algorithms can and cannot do.

On the experimental side, ITL has impressive laboratories for quantum components and systems development, quantum metrology, and metrology for quantum networks. ITL is part of a major effort of the NIST Gaithersburg Quantum Network (i.e., NG-QNet) Testbeds, which is a suite of testbeds being built on the NIST Gaithersburg campus to implement and characterize various aspects of quantum networks, consisting of a large collaboration with various NIST laboratories and other federal agencies. On the development of quantum systems and control, an example of a high-impact work is a publication on advances in automation of quantum dot device control in *Review of Modern Physics*, the most prestigious journal in physics (Zwolak and Taylor 2023).

Other portfolio projects at ITL include the advancement of Neuromorphic AI, which aims to develop computational systems that directly mimic the brain and to use these systems for AI.

The Visualization Laboratory has capabilities for both 2D and 3D visualization. Projects demonstrated within a virtual reality cave environment interacted with advanced application areas ranging from health to civil engineering. The work has had a tremendous impact on scientific visualizations through the integration of the Immersive Visualization Environment with Paraview, a widely used fully open-source software environment, and their ongoing efforts toward the development of standards for extended reality.

## Opportunities and Challenges

Explicit information on any sort of a strategic plan for ACMD was lacking. A strategic vision for this division's work was partially reflected in the presentations, but it could be communicated more explicitly and in a more coherent and systematic manner. Developing a strategic plan would serve to connect and cohere the diverse portfolio of projects in line with present and estimated future trends, link and position changes in response to external demands and mandates, and adapt to the emergence of new topics and the potential obsolescence of current topics. This would help with consolidating the project portfolio into fewer key strategic initiatives and staffing them appropriately within the current budget constraints, providing a method for preventing project fragmentation, and avoiding the creation of projects that are not aligned with, and divert resources from, the strategic goals of the division.

> **Recommendation 4-1: The Applied and Computational Mathematics Division should develop a strategic plan, derived from its strategic vision, to focus its efforts and resources on what have been determined to be the most important lines of work and to prevent the establishment of projects that are not aligned with the strategic vision and that would diffuse the division's resources and reduce its impact.**

AI will have numerous and perhaps significant impacts on ACMD's work. Examples of high-impact potential opportunities include the use and development of large language models to support mathematical discovery (e.g., theorem proving), neuro-symbolic strategies, and conversely, how to deploy the expertise and resources of the division to improve the performance of large language models.

ACMD needs to develop a more ambitious AI strategy specific to ACMD's aims. In addition to AI supporting and improving mathematical modeling, the infrastructures, tools, and methods are critical in an AI context need to be addressed. The key strategic areas of involvement and opportunities for national and international leadership within the AI space need to be identified.

Copyright National Academy of Sciences. All rights reserved.

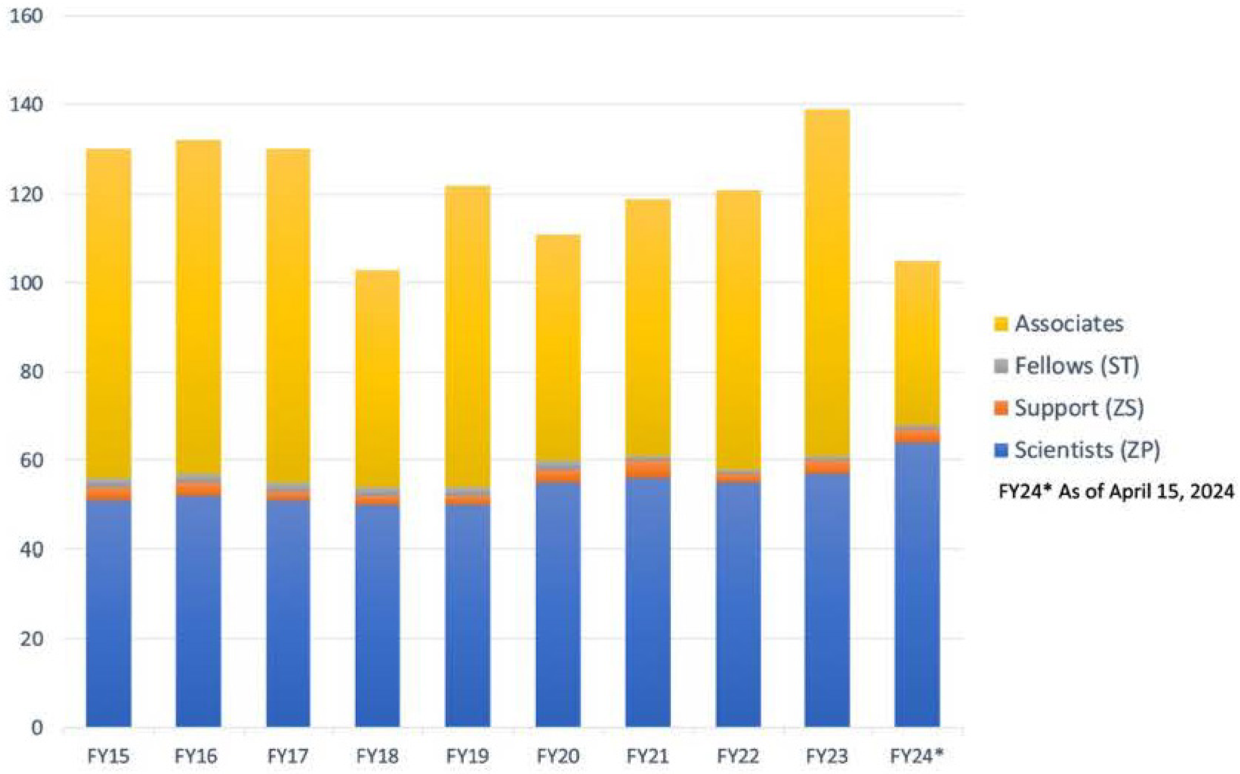


**FIGURE 4-1** Applied and Computational Mathematics Division staffing from fiscal year (FY) 2015 through FY 2024.
SOURCE: Courtesy of NIST Information Technology Laboratory.

**Recommendation 4-2: The Applied and Computational Mathematics Division should develop a strategic plan that reflects an integrated vision of the impact of artificial intelligence (AI) on the division, both the short and long term. This plan should address critical questions such as the following:**

**a. How can AI support and improve productivity for mathematical modeling?**
**b. Which infrastructures, tools, and methods are critical within this context?**
**c. What are the key strategic areas of involvement and opportunities for national and international leadership within the AI space?**

## ASSESSMENT OF SCIENTIFIC EXPERTISE

ACMD currently has 62 federal employees. Of these, 56 hold PhDs, 52 are full-time, and 48 hold permanent appointments. There are 14 term appointees, including 6 National Research Council postdoctoral researchers. There are 46 associates, including 30 guest researchers (of whom some are postdoctoral researchers), 2 Professional Research and Experience Program postdoctoral researchers; 2

Copyright National Academy of Sciences. All rights reserved.

contractors; and 12 students.[1] The staffing levels have fluctuated between fiscal year (FY) 2015 and FY 2024. These levels are shown in Figure 4-1.

ACMD encompasses technical expertise in an outstandingly large number of areas of applied mathematics and computational science and has applied this expertise to an equally impressive number of application domains, balancing broader mathematical modeling areas and more specific focal areas such as quantum computing and communication, with a good balance between core mathematical modeling and applications to practical and industrial settings. The contributions within the division have a distinctive set of characteristics—namely, (1) the ability to flexibly approach a diverse spectrum of problem spaces and domains that require mathematical modeling expertise, (2) the ability to sustain long-term efforts for the construction of high-quality data and software resources, and (3) the capacity to balance a diversified portfolio of contributions as a service to other divisions across NIST while promoting its internal strategic areas. This diversity of expertise enables ACMD to engage with and support both internal and external partners in a diverse spectrum of collaboration areas, as well as to develop and sustain its research agenda.

## Accomplishments

The portfolio of projects presented at the meeting showed unambiguously the technical quality of the scientific expertise within ACMD. Most notably, this is a unique team that integrates diverse and complementary scientific expertise areas such as the following:

- A set of long-term strategic research programs that have a claim to national and international research leadership, most notably in quantum algorithms, quantum cryptography, and quantum networks.
- The Digital Library of Mathematical Functions and OOMMF, which comprise a set of long-term resources and data sets that have visibility, impact, and an engaged community.
- A diverse portfolio of projects within high-impact application areas that requires a diverse and deep set of mathematical modeling skills—for example, contributions to standards for Body Area Networks in IoT-Health, analysis tools for better discrimination of drug compounds, and development of federal standards for post-quantum cryptography.

The staff collectively hold several distinctions, including

- American Association for the Advancement of Science fellow
- Association for Computing Machinery fellow
- American Statistical Association fellow
- American Physical Society fellow
- Washington Academy of Sciences fellow
- NIST fellow
- QuICS fellow

The staff collectively also hold several awards, including

- Department of Commerce Ron Brown Award
- Department of Commerce Gold Medal
- Department of Commerce Silver Medal
- Department of Commerce Bronze Medal

[1] Associates are not NIST employees. They are outside researchers, both foreign and domestic, who collaborate with NIST researchers.

Copyright National Academy of Sciences. All rights reserved.

- Washington Academy of Sciences Excellence in Research in Applied Mathematics Award

### Opportunities and Challenges

Given the rapid progress in generative AI and its impact on a widespread range of applications, ACMD would benefit from having more expertise in the AI area, whether through new hires or proactively upskilling its employees. Having some AI researchers and engineers on the staff will enable ACMD to adapt to the latest technology and to stay current on developments in this rapidly evolving field. While recruiting permanent staff can be a long-term option, establishing a contractor-based or visiting researcher program could be a sensible short-term option to support a more agile knowledge transfer in this domain. This would enable the division to identify new opportunities for integrating contemporary AI methods such as large language models with its existing research workflows.

> **Recommendation 4-3: The Applied and Computational Mathematics Division should expand the artificial intelligence (AI) expertise available to it. In the long term, it should add AI researchers and engineers. This can be accomplished through new hires, upskilling existing staff, or both. Until it can bring on permanent staff in this area, the division should establish a contractor-based or visiting researcher program to support a more agile knowledge transfer in this domain. These programs might help identify candidates for hiring.**

## BUDGET, FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

### Budget

The largest share of ACMD's funding comes from scientific and technical research services appropriations. Other contributions include Innovations in Measurement Science—which is an internal NIST competitive grant program to fund NIST researchers to improve NIST's capabilities, Strategic and Emerging Research Initiatives funding, and funding it receives for work done for other federal agencies. ACMD's budget increased from approximately $15 million in FY 2015 to approximately $20 million in FY 2024. Figure 4-2 shows the ACMD budget each year between FY 2015 and FY 2024. Figure 4-3 shows the breakdown of the FY 2024 ACMD budget.

### Facilities and Equipment

ACMD has access to state-of-the-art laboratories, including a data visualization laboratory with a virtual reality cave and laboratories for quantum network experimentation. A significant emphasis of the group is on mathematical modeling and software development. The environment addresses these needs with a mixture of private and shared workspaces and a portfolio of small and large meeting spaces.

Much scientific work happens in the moment, not on a schedule. Despite the general fit of the current physical infrastructure to the work being done, there is a lack of available meeting spaces for remote meetings and other conferences, whether over calls or in person, that can be used without a need for advanced scheduling. Acknowledging that office space is limited, it would be beneficial to designate rooms that researchers can reserve for remote meetings and other conferences with researchers without the need for advanced scheduling.

> **Recommendation 4-4: The Applied and Computational Mathematics Division should designate rooms that its staff can use for remote meetings and remote and in-person conferences with other researchers without the need to schedule them in advance.**

Copyright National Academy of Sciences. All rights reserved.

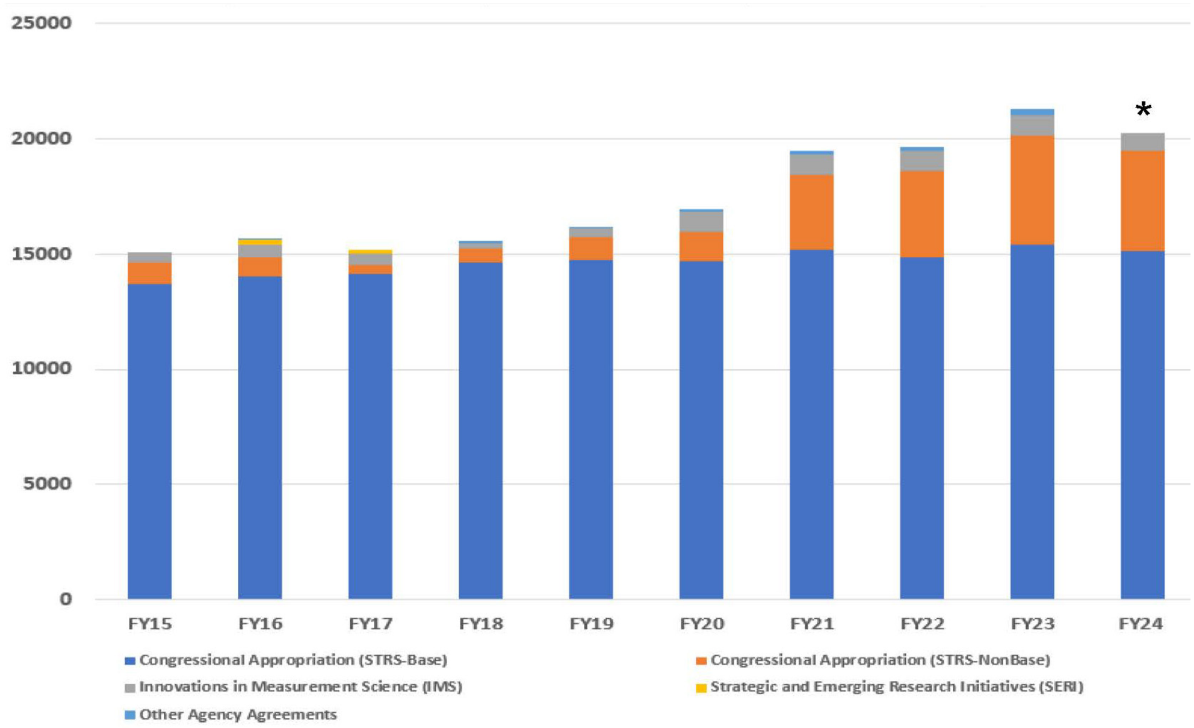
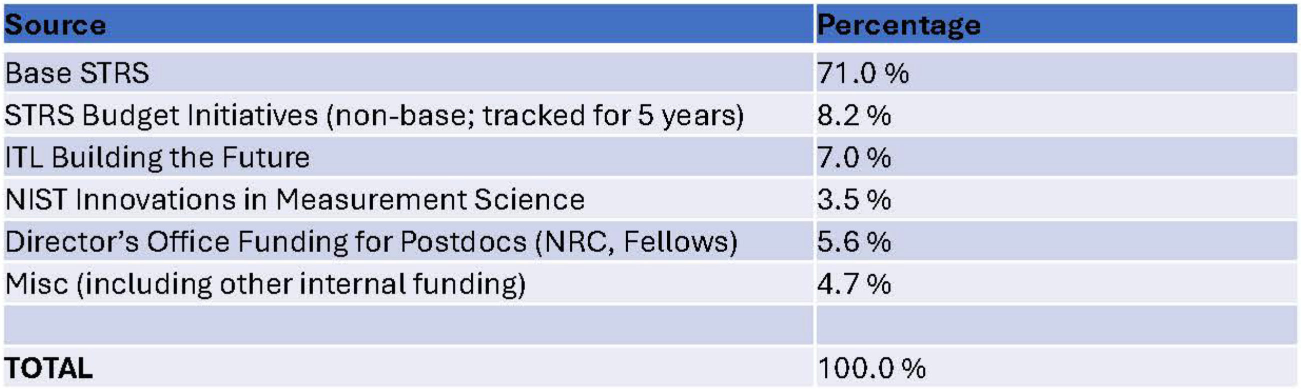


**FIGURE 4-2** Applied and Computational Mathematics Division budgets from fiscal year (FY) 2015 to FY 2024.
NOTE: STRS, scientific and technical research services.
SOURCE: Courtesy of NIST Information Technology Laboratory.



| Source | Percentage |
|---|---|
| Base STRS | 71.0 % |
| STRS Budget Initiatives (non-base; tracked for 5 years) | 8.2 % |
| ITL Building the Future | 7.0 % |
| NIST Innovations in Measurement Science | 3.5 % |
| Director’s Office Funding for Postdocs (NRC, Fellows) | 5.6 % |
| Misc (including other internal funding) | 4.7 % |
| | |
| **TOTAL** | 100.0 % |

**FIGURE 4-3** Applied and Computational Mathematics Division budget breakdown for fiscal year 2024.
NOTE: ITL, Information Technology Laboratory; NRC, National Research Council; STRS, scientific and technical research services.
SOURCE: Courtesy of NIST Information Technology Laboratory.

Copyright National Academy of Sciences. All rights reserved.

### Human Resources

It is clear that ACMD is attractive for recruiting and retaining staff. Discussions with permanent staff indicated that the reasons for this include general job security; significant research independence; diversity of technical challenges; focus on research without a substantial teaching, administration, or funding acquisition workload; and a collaborative research environment. For nonpermanent junior staff, the reported benefits include a rich technical environment and the possibility of long-term retention and mentoring.

The panel identified two opportunities for improvement. The first is anticipating the medium- and long-term strategic demands of the division that could align with future permanent positions and or contract extensions. The second is aligning the timing of the postdoctoral researcher recruitment process with the corresponding academic timelines.

## EFFECTIVENESS OF DISSEMINATION EFFORTS

Between October 2022 and December 2023, ACMD staff produced 61 papers in peer-reviewed journals, 39 papers in conference proceedings, and 6 publications in various other venues. In addition, 17 papers had been accepted for publication and 40 were in review. ACMD staff gave 79 invited talks and 74 talks at conferences and workshops.

The staff are widely engaged with stakeholders, holding 11 journal editorial positions and 30 positions on various conference committees, and memberships in several organizations, including the following:

- Society for Industrial and Applied Mathematics Board of Trustees
- White House Office of Science and Technology Policy’s Working Group on Quantum Networks
- White House National Science and Technology Council’s Subcommittee on Future Advanced Computing Ecosystem
- World Wide Web Consortium Advisory Committee
- World Wide Web Consortium Math Interest Group
- Tcl Core Team
- International Federation for Information Processing WG 2.5 (Numerical Software)
- IEEE 802.15 Task Group 6ma (Body Area Networking)
- Khronos OpenXR Working Group

### Accomplishments

ACMD’s software packages have had a broad reach, with evidence of having a broad impact. OOMMF is used for micromagnetic modeling. It was downloaded 5,200 times by 3,300 clients in 2023. Overall, this software package has been cited more than 3,700 times, including in 25 dissertations and 45 U.S. patent applications. There are more than 30 YouTube tutorials for this software package, and it is on nanoHub.

OOF,[2] used for modeling material microstructures, is also available on nanoHub. It was exercised 4,300 times in 2023 and has been exercised a total of 69,000 times since 2007. The current version is OOF2, and OOF3D is also available.

Automated Combinatorial Testing for Software, known as ACTS, has been downloaded by 4,775 distinct users since 2014.

[2] This is known simply as OOF. For more information, see NIST (2023).

Copyright National Academy of Sciences. All rights reserved.

Other software that is in development or being distributed includes

- LaTeXML, a TeX/LaTeX to HTML/MathML converter
- Scikit-shape, a Python package for shape and image analysis
- G2Aero, a Python package for separable shape tensors
- Software for Joint Quantum State Tomography

In 2023, there were more than 14.3 million requests to the division's web server by more than 940,000 visitors. The Digital Library of Mathematical Functions saw 5.1 million pages downloaded by 351,000 unique visitors and has been cited more than 10,000 since 2010. Other ACMD data being distributed includes Dark Solitons in Bose-Einstein Condensates data set, which supports machine learning, and QFlow, quantum dot data for machine learning.

The Handbook of Mathematical Functions has been a worthy, widely disseminated project. Its continued maintenance would be of great benefit to the broader mathematical community.

### Opportunities and Challenges

The development of other reference materials like the Handbook of Mathematical Functions for the broader mathematical community might be another line of work suitable for ACMD.

**Recommendation 4-5: The Applied and Computational Mathematics Division (ACMD) should maintain the Handbook of Mathematical Functions. ACMD should consider whether the division wants to develop new reference materials for the mathematical community.**

A significant part of the work of the division is attractive to an audience beyond the usual stakeholders. While NIST has a Public Affairs Office and ACMD engages with it, it is unclear whether the current communication channels and processes are sufficient to provide adequate visibility of ACMD's work to external stakeholders and others who may be interested in it.

While researchers do engage with the academic community and with the Department of Commerce more broadly, the strategy for communicating with external stakeholders is not clear. Some critical questions to address include the following: What are the other communities to which the division's work needs to be visible (e.g., Congress, industry, education, or citizens)? What are the positive outcomes that can emerge from a broader engagement (e.g., increased funding and better access to human resources)? What communications channels are most accessible to these communities (e.g., events, videos, or textual content)? What is ACMD's web presence strategy? What resources are required to deliver the best possible communication outcomes?

Last, dissemination metrics are based on numbers: of publications, downloads, and page views, for instance. This is a measure of reach. Metrics that can be used to measure and, critically, communicate impact to stakeholders and appropriators would be very useful but seem to be lacking.

**Recommendation 4-6: The Applied and Computational Mathematics Division (ACMD) should develop a strategy for the improved communication of its work to stakeholders. ACMD should also develop additional metrics to better illustrate the impacts of its ongoing work.**

## REFERENCES

NIST (National Institute of Standards and Technology). 2023. "OOF: Finite Element Analysis of Microstructures." Updated September 8. https://www.ctcms.nist.gov/oof.

Zwolak, J.P., and J.M. Taylor. 2023. "Colloquium: Advances in Automation of Quantum Dot Devices Control." *Review of Modern Physics* 95:011006. https://doi.org/10.1103/RevModPhys.95.011006.

Copyright National Academy of Sciences. All rights reserved.

# 5
# Computer Security Division

The Computer Security Division (CSD) concentrates on near-term issues. That is, it deals with existing problems or issues reasonably believed to be likely problems in the foreseeable future. This does not imply that the solutions are easy or obvious or even "mere" engineering. Not only are deep insight and creativity needed to solve these problems, but a fair amount of political and interpersonal skill is needed to get these solutions accepted and, in some cases, even developed.

The panel received presentations on CSD as a whole and on a number of different projects being carried out within the division. The latter include groups working on cryptographic technology, security test validation and measurement, security components and mechanisms, secure systems and applications, post-quantum cryptography (PQC), trustworthy artificial intelligence (AI), the National Vulnerability Database, cryptographic module validation, protection of unclassified information, lightweight cryptography (LWC), hardware security, security guidance for microservices-based architectures, and risk management frameworks.

Not every project presented to the panel is discussed in the report. Only those projects about which the panel had comments are discussed.

## ASSESSMENT OF TECHNICAL PROGRAMS

### Accomplishments

*Cryptographic Technology Group*

Over the past 10 or so years, cryptographic technology has been a growth area for CSD. Apart from the need for new standards, such as for post-quantum algorithms, in response to past situations where a lack of in-house cryptography expertise was a problem CSD has significantly strengthened the cryptography expertise resident on staff. CSD now has adequate cryptography expertise on staff, and the division has established its credibility in this area of expertise, most recently culminating in the hosting competitions in post-quantum cryptography and light-weight cryptography.

The Cryptographic Technology Group is doing work that is probably without peer in the world. Its algorithms, although technically required only for unclassified U.S. government systems, are more widely used than any competing national or international standards, including within the European Union, which often has its own equivalents. Many of the products of this group, such as the Advanced Encryption Standard (AES) and the newest version of the Secure Hash Algorithm (SHA), have been products of open, worldwide competitions. It is notable that the winners of these competitions that have since been standardized—AES and SHA-3—were algorithms submitted to the competition by Europeans.

Other major work areas for the cryptography technology group include PQC, zero-knowledge proofs, and modes of operation. Foreign researchers often visit; this is good for establishing links to other national standards bodies.

About half of the staff of the Cryptographic Technology Group is working on PQC algorithms, algorithms that are designed to be resistant to attack by future quantum computers. The ongoing PQC program is a jewel in the Information Technology Laboratory's (ITL's) crown. The deliberate

Copyright National Academy of Sciences. All rights reserved.

establishment of in-house mathematical expertise; the open, transparent, and fair competition; the measured pace; the curation of community; and the professionalism of the project management have all combined to form a widely supported and successful cryptographic algorithm competition. All currently used public-key algorithms, including Rivest-Shamir-Adleman (RSA), Diffie-Hellman, and the elliptic curve equivalents, will be vulnerable to attack by quantum computers once powerful enough quantum computers—that is, ones with a sufficient quantity of quantum bit-equivalents (qbits)—are built. While it is not clear when such computers will become practical, a lot of existing data will need to be protected for many years, perhaps decades. Accordingly, there is an urgent need for new PQC algorithms now, to guard against forged signatures and decryptions of recorded traffic in the future.

CSD responded by hosting a competition to develop PQC algorithms. As with all CSD's cryptographic competitions, this one started with a statement of requirements and an open call for public submissions. There followed a sequence of public workshops to discuss the various submissions, followed by an evaluation of each candidate algorithm in light of the research results attacking or supporting each remaining candidate PQC algorithms. At the conclusion of each round of the evaluation, some candidate algorithms were dropped and others were passed on to the next round for further consideration.

As of the panel's review, the PQC competition had completed five rounds and was almost done. It is considered relatively high risk because the criteria for creating and attacking post-quantum cryptographic algorithms are not as well developed as for older, pre-quantum technologies. CSD has dealt with this by selecting backup PQC algorithms, in case an unforeseen attack should be developed later. The current surviving candidates all appear to have strong support worldwide.

This ongoing work, along with the unpredictable pace of adversarial technology and mathematical developments, means that ITL will have to remain capable in PQC matters for some time to come.

Traditional cryptographic algorithms like AES are often too resource-intensive for devices with limited computational power, memory, and energy resources. Despite these constraints, such devices still require strong security measures to protect sensitive data and ensure privacy and integrity.

LWC is intended for resource-constrained devices such as smart home devices, connected cars, smart cards, radio frequency identification tags, pacemakers, and Internet of Things (IoT) devices. CSD has initiated the LWC Standardization Process, an open competition, similar to the SHA-3 and the much older AES competitions, to address the growing need for cryptographic standards tailored to constrained environments.

CSD announced a LWC competition in 2018. The competition aimed to identify and standardize lightweight cryptographic algorithms that could provide adequate security and resource efficiency for resource-constrained environments and promote research and development in the field of LWC. It consisted of multiple rounds, each involving rigorous analysis by CSD and the cryptographic community, leading to a progressively narrower selection of candidates. Public workshops, conferences, and comment periods allowed for broad community involvement. The competition concluded with the selection of the Ascon family of algorithms as the standard for LWC applications and the decision was announced in February 2023. This competition represents a significant effort to address the unique security needs of resource-constrained environments by fostering innovation and rigorous evaluation. The competition's outcomes have far-reaching implications for the security of IoT devices and other applications where traditional cryptographic algorithms are impractical.

### *Security Testing, Validation, and Measurement Group*

The Security Testing, Validation, and Measurement Group focuses on developing, implementing, and promoting security standards and guidelines. This group is instrumental in ensuring the security and reliability of information systems through rigorous testing, validation, and measurement techniques. Its activities can be listed in the following five sub-categories:

Copyright National Academy of Sciences. All rights reserved.

1. The Cryptographic Module Validation Program validates cryptographic modules to ensure they meet the Federal Information Processing Standards (FIPS) and other National Institute of Standards and Technology (NIST) standards. This program aims to ensure that cryptographic modules used in federal systems are secure and comply with standards such as FIPS 140-2 and FIPS 140-3, both titled "Security Requirements for Cryptographic Modules. These modules are validated by laboratories accredited by CSD and the National Voluntary Laboratory Accreditation Program."[1] ITL is resourced by the laboratories and the National Voluntary Laboratory Accreditation Program to support this activity.
2. The Cryptographic Algorithm Validation Program provides validation testing for cryptographic algorithms to ensure they are implemented correctly. Its scope includes all NIST-approved algorithms including AES, SHA, RSA, Digital Signature Algorithm, and elliptic curve cryptography.
3. The Security Content Automation Protocol is a suite of specifications used to automate vulnerability management, vulnerability measurement, and policy compliance evaluation. This protocol helps organizations manage security risks by automating the process of checking systems against security policies and configurations. Its components include standards such as Common Vulnerabilities and Exposures, Common Configuration Enumeration, and eXtensible Configuration Checklist Description Format.

The activities of the Security Testing, Validation, and Measurement Group are crucial for ensuring that cryptographic products and algorithms used in government and industry meet stringent security standards, providing a framework for continuous improvement in security practices through rigorous testing and validation, and promoting interoperability and reliability in security technologies across different sectors.

### *Security Engineering and Risk Management Group*

Standards and guidelines developed and published by the Security Engineering and Risk Management Group help to improve the security of information systems. Examples are FIPS publications, NIST Special Publications such as SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and SP 800-57, "Recommendation for Key Management."

### *Security Components and Mechanisms Group*

The Security Components and Mechanisms Group is involved in several key initiatives aimed at system security, metrology, emerging technologies, and cybersecurity management. The key achievements listed in the group presentation are all in areas of AI—specifically,

- Trustworthy AI,
- Taxonomy of attacks and mitigations in AI,
- AI models used in autonomous vehicles, and
- Measuring and evaluating the efficacy of AI.

As part of its AI activities, the Security Components and Mechanisms Group has

[1] The National Voluntary Laboratory Accreditation Program is part of the NIST Standards Coordination Office in the Associate Director for Laboratory Programs Office. It accredits laboratories to perform specific tests and calibrations, including those related to cryptographic module testing, ensuring that laboratories meet the necessary qualifications to conduct rigorous and accurate testing. For CSD, it accredits laboratories that support the Cryptographic Algorithm Validation Program.

Copyright National Academy of Sciences. All rights reserved.

1. Developed the Secure Software Development Framework in support of Executive Order 14110, “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”
2. Developed the new NIST AI 100-2 E2023, “Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations,” which was widely adopted across industry, media, and governments and has been the basis for the upcoming standard AI 100-2A.
3. Developed an “eye test” for computer vision models.
4. Developed an AI measurement and evaluation platform.

In addition to AI-related activities, the Security Components and Mechanisms Group has also developed SP 800-223, “High-Performance Computing Security: Architecture, Threat Analysis, and Security Posture,” in support of Executive Order 13702, “Creating a National Strategic Computing Initiative.” Another important contribution of the Security Components and Mechanisms Group is the development of FIPS 201-3, “Personal Identity Verification (PIV) of Federal Employees and Contractors.”

### *Secure Systems and Applications Group*

The Secure Systems and Applications Group has been focusing on attribute-based access control. This is a reasonable idea, but the concepts are at least 25 years old. Although attribute-based access control has been widely adopted by industry over the years, it is unclear where the market is today. This group has leveraged its strong past success in attribute-based access control to develop novel and advanced access control solutions. They have extended their expertise to support access control in zero-trust architecture: standards-based access control is not currently supported in existing products. It is a gap in industry because it requires integration across different components of zero-trust architectures, but different vendors have different strategies. Vendor lock-in is the strategy for large providers, so they have little incentive to build systems with open architectures where components can be replaced by those from other vendors, while acquisition by a larger vendor is the strategy of small ones. Government work in this zero-trust gap is directly applicable to Executive Order 14028, “Improving the Nation’s Cybersecurity,” and is not in competition with anything industry is pursuing. In addition, the Secure Systems and Applications Group has found a technology transition partner, which positions them well to be the leaders in standards of integration in this zero-trust gap area. However, owing to vendor strategies, it is not entirely clear how much impact the effort on the zero-trust initiatives will have nationally and internationally. The service mesh work presented did not include any metrics for success.

### *National Vulnerability Database*

The National Vulnerability Database (NVD) is one of the key programs presented to the subpanel. From a technology development perspective, the NVD program has been a great success, in large part owing to the leadership provided by the federal employees assigned to the program. That said, it is a crucial security resource that is consuming a significant amount of resources, largely for Amazon Web Services fees for making the data available. These costs are likely unsupportable in light of the limited resources available to CSD.

Today, the NVD can be accessed by a legacy database download method and an application programming interface (API). The database download is an old and expensive method—users have to transfer everything, rather than just what they need. The API is less expensive to operate. CSD is trying to move away from the legacy database download method to using only API access but has been unsuccessful in doing so to date. It was reported to the panel that what is lacking seems to be a decision to finally make the change.

**Recommendation 5-1: To increase security, automate as much of the workload as possible, and reduce operating costs, the Computer Security Division should migrate access to the**

Copyright National Academy of Sciences. All rights reserved.

**National Vulnerability Database to an application programming interface as rapidly as possible.**

*Security Guidance for Microservices-Based Architectures Group*

The Security Guidance for Microservices-Based Architectures Group develops security architecture standards. It operates at a much lower functional level and so does not use the access control framework being developed by the Secure Systems and Applications Group. Companies regularly claim that their chips are resistant to hardware, or side-channel, attacks, but there are no common criteria for judging the resistance. The private sector is unlikely to achieve consensus on any common criteria or standards because they will develop and market product-specific security architecture standards to highlight their particular security features. ITL's and CSD's work in this area provides an independent and trusted security architecture standard to which industry can conform, increasing confidence in the security of hardware.

### Opportunities and Challenges

The Security Components and Mechanisms Group is doing excellent work, but their scope may be too ambitious for the available resources.

It might be useful for the Security Guidance for Microservices-Based Architectures Group to use competitions, like those for PQC and LWC, to prompt the development of security architecture standards.

It is not entirely clear what criteria are used to define projects or how projects are prioritized. It is also not clear how CSD decides that a project has been successful and should be retired. CSD is overcommitted and, especially in light of the budget discussion below, does not have the resources to continue its current suite of projects at sufficient depth to lead to groundbreaking results. Also, some groups do not seem to understand the larger purpose of their work nor how it fits into the larger CSD vision, although CSD leadership does seem to understand this. More coordination, closer mentoring, and cross-group interaction would be helpful. There also appears to be a need for strategic planning of work to intentionally consider what projects should be pursued with CSD's very limited resources, how they fit into CSD's mission, and when projects ought to be retired in favor of new work.

**Recommendation 5-2: The Computer Security Division (CSD) should engage in a strategic planning process to intentionally choose projects that align with its mission and make the best use of the division's extremely limited resources. This plan should also consider when projects have been successful and what projects ought to be retired to free up resources for new work. This plan should be clearly communicated to all CSD staff so that they understand exactly how their work fits into the broader divisional mission.**

The Cryptographic Module Validation Group publishes a list of validated modules, but not in a form that can be easily parsed by machine. This limits the impact of this list. CSD has a portfolio of programs that started at low volumes and were supported manually. Examples are the NVD and the Cryptographic Module Validation Program. Each of those programs has seen wide adoption. The volume of work has increased to outstrip the resources available, resulting in unacceptably long wait times for validation and compromising their value to users and the nation. The challenge is to operate at scale through advanced planning for success, timely development of automated processes, and resourcing the appropriate mix of staff skills. The skills necessary to conceive and create a program are generally different from the skills necessary to sustain it and operate it at scale. There is an opportunity to free the creators from a successful program so that they are available to create new things. In short, CSD excels at developing technologies, but ought not be an operational agency. Once a technology has been developed, it is advisable to hand it off to someone else to operate, such as contractors who specialize in operations versus research and creation. This has been done successfully with cryptographic module validation but not with the NVD.

Copyright National Academy of Sciences. All rights reserved.

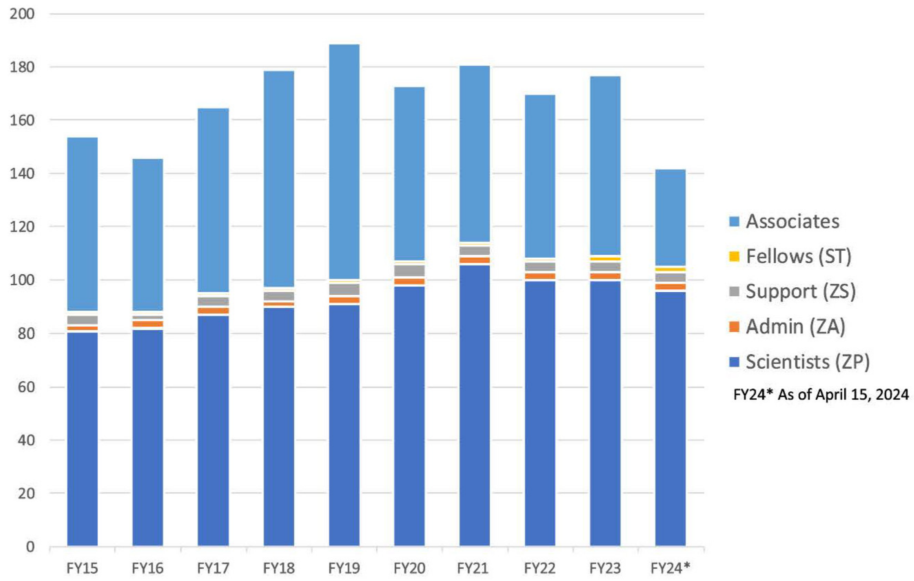


**FIGURE 5-1** Computer Security Division staffing levels from fiscal year (FY) 2015 through FY 2024. SOURCE: Courtesy of NIST Information Technology Laboratory.

> **Recommendation 5-3: To free up staff and financial resources for new work, the Computer Security Division should hand off developed technologies to others such as contractors to operate. This will allow researchers to focus on what they are good at and put operations in the hands of those who are skilled at it.**

CSD provides several free public goods whose provision might be monetized to create revenue streams and offset costs, reducing financial stresses (see the section “Budget,” below). These goods include patent licenses and access to online services, including the wildly successful NVD and the Cryptographic Module Validation Program. Much as other NIST laboratories charge for standard reference materials and reference data sets, perhaps CSD could charge commercial organizations that build commercial products on top of the NVD some fee for using the service, helping to offset some of the costs associated with maintaining this database. Individual and noncommercial access to the NVD, however, would need to remain free. It is advised that cost recovery for commercial use of such services be aggressively computed to include not only computing and storage but also the fully burdened staff costs of creating, automating, and providing these services.

## ASSESSMENT OF SCIENTIFIC EXPERTISE

As of May 2024, CSD had 140 staff. There are 86 scientists, 44 associates, 2 fellows, 5 support staff, and 3 administrative staff.[2] Figure 5-1 shows CSD staffing levels and composition from fiscal year (FY) 2015 through April 15, 2024.

[2] Associates are not NIST employees. They are outside researchers, both foreign and domestic, who collaborate with NIST researchers.

Copyright National Academy of Sciences. All rights reserved.

### Accomplishments

The quality of the CSD staff is reflected in the wide range of professional awards and honors they have received. A sampling includes

- Department of Commerce Gold Award
- Department of Commerce Silver Award
- Women in Technology Rising Star Award
- Washington Academy of Sciences Distinguished Career Award in Computer Science
- 2023 NIST George A. Uriano Award
- 2023 IEEE International Conference on Software Testing, Verification and Validation Most Influential Paper Award
- Washington Academy of Sciences fellow

The CSD staff are generally world-class in their areas, leading cutting-edge work. For example, the Cryptographic Technology Group organizes and leads open competitions for cryptographic algorithms, including PQC. These competitions attract wide participation from academia and industry. The entrants present their solutions while critiquing the entries of others. The arguments on all sides are deeply technical and mathematical. CSD staff sort through all this using their organic expertise to reach sound and defensible decisions. These lead to standards that form the basis for secure communication worldwide in support of internet access, e-commerce, wireless infrastructure, and personal privacy. The staff are go-to experts in their areas.

The group working on access control issues is similarly well respected. Their work on biometrics, and in particular their measurements of accuracy and bias in various algorithms, plus their standard data set, are used worldwide. Their newer work on attribute-based access control holds great promise for the future: it is one of very few implementations of the concept, and their algorithm and programs for converting attribute graphs to industry-standard access control lists make the work extremely portable and valuable. Similarly, the extension of attribute-based access control to cloud and zero-trust architectures will be extremely valuable.

In general, CSD does not have any obvious gaps in the expertise represented by its staff. CSD generally hires staff to meet expertise needs. Any of them could easily find a job in industry and NIST is fortunate to have them.

### Opportunities and Challenges

The CSD staff is expanding to meet the security needs of the CHIPS and Science Act of 2022 (P.L. 117-167). There is an opportunity to expand the cryptography acceleration and side-channel analysis team with new expertise and staff.

## BUDGET, FACILITIES, EQUIPMENT, AND HUMAN RESOURCES

### Budget

CSD’s budget from fiscal year (FY) 2015 through FY 2024 is shown in Figure 5-2. STRS is the scientific and technical research services appropriation that funds the laboratory’s technical work. Innovations in Measurement Science is an internal NIST grant program to fund work to advance metrology. The Strategic and Emerging Research Initiatives program is an internal NIST effort to fund work to perform research studies to identify issues and opportunities in measurement science, trustworthiness, and innovation. Other agency agreements represent reimbursable work done for other federal agencies.

Copyright National Academy of Sciences. All rights reserved.

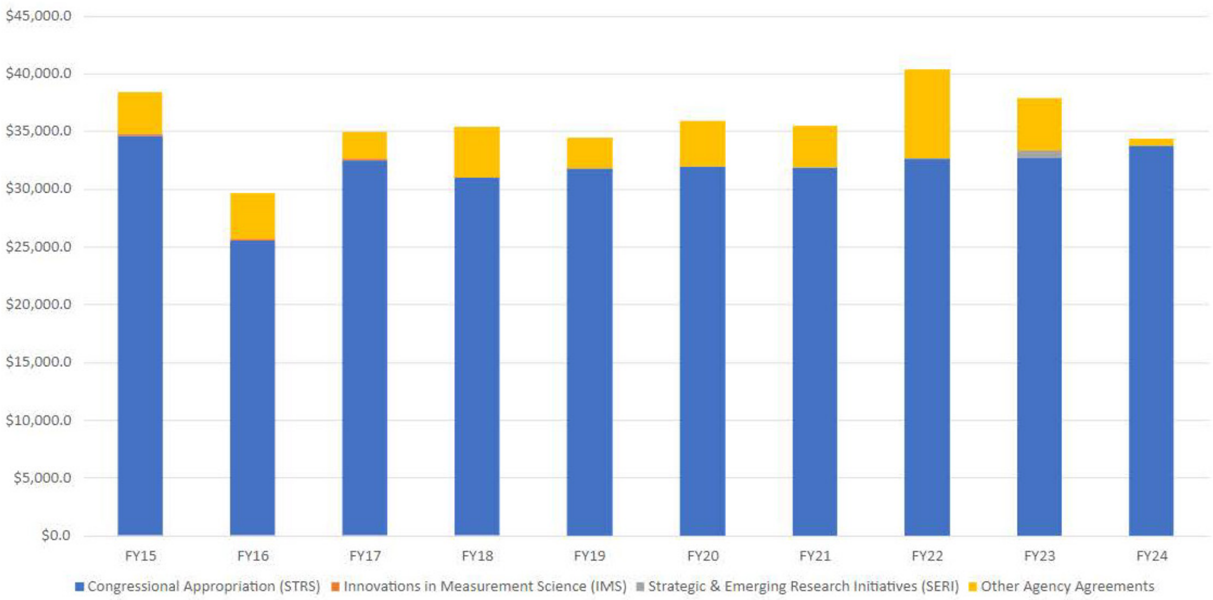


**FIGURE 5-2** Computer Security Division budgets from fiscal year (FY) 2015 through FY 2024.
NOTE: STRS, scientific and technical research services.
SOURCE: Courtesy of NIST Information Technology Laboratory.

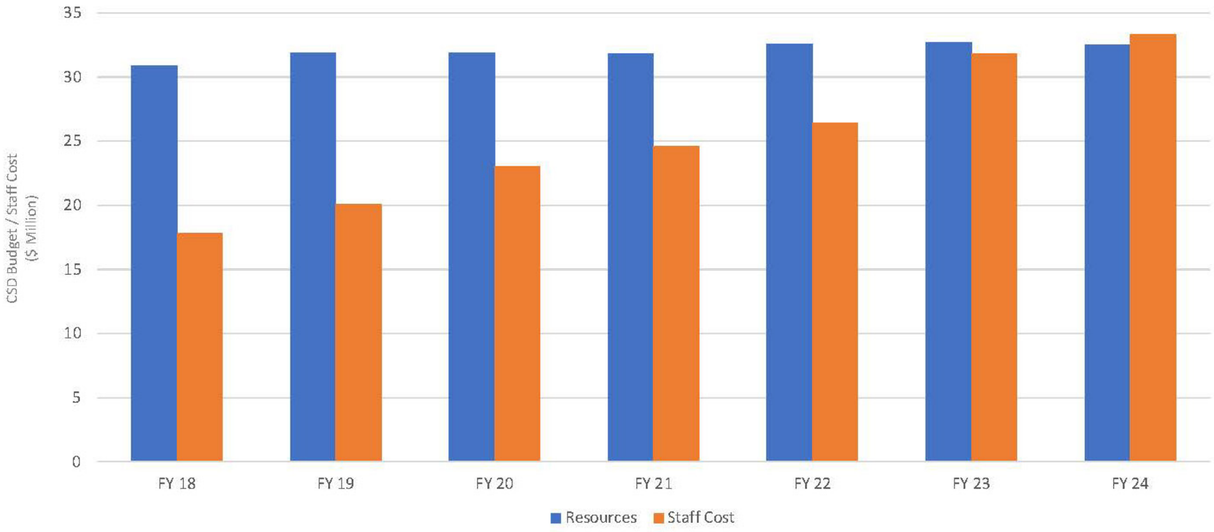


**FIGURE 5-3** Computer Security Division (CSD) staff cost growth versus appropriations for fiscal year (FY) 2018 through FY 2024. The resources are the scientific and technical research services appropriations only and the staff costs are for full-time equivalents only.
SOURCE: Courtesy of NIST Information Technology Laboratory.

Copyright National Academy of Sciences. All rights reserved.

As can be seen, the budget has fluctuated holding largely at around the $35 million level for most years in this span. The budget for FY 2024 is $4 million less than that for FY 2015, so there has been a real decrease in the budget over this time. It is important to note that these numbers are not corrected for inflation, so it is very likely that CSD has lost ground in its budget over the past decade.

The budget picture, however, becomes bleaker when the CSD budget is compared with the salary growth of its staff. Staff members usually receive annual raises, and some NIST laboratories have adjusted salaries to make them more competitive with the private sector. Figure 5-3 shows how staff costs have grown compared with CSD's baseline congressional appropriations between FY 2018 and FY 2024. The costs are for full-time equivalents only.

The relatively flat budgets over the past decade, inflation, and the growth in staff costs taken together mean that CSD faces a budget crisis. Its budget has been flat or declining in recent years, and as a consequence recruitment has been hard of late. Congressionally allocated funds no longer cover even the raw staff costs. Travel, which is necessary to establish and maintain relationships to influence standards, is no longer funded. Contractors, who are required to operate successful programs at scale, are no longer funded. Student intern programs, necessary to build the workforce, are no longer funded. CSD's work is not sustainable at current levels of funding.

### Facilities and Equipment

Unlike most other NIST laboratories, ITL does not require facilities with precise environmental controls or a wide range of expensive and sensitive equipment. ITL does need computers and server rooms with proper environmental controls. CSD has these. The panel noted no deficiencies in the facilities or equipment that CSD uses.

### Human Resources

The main human resources challenge facing CSD is the aging workforce. Many people are retirement-eligible or will be soon. Morale is generally high, and many people stay well past retirement. But the problems caused by inadequate resources vis-à-vis hiring new staff as discussed earlier in the section "Budget" cannot be underestimated. A consequence of this is the lack of a deep bench; the senior staff are excellent but do not have adequate backup because of the inability to hire newer junior staff.

If, as CSD is contemplating, they institute a retirement incentive program to cut salary costs, this will result in a skill gap and a lack of mentoring for junior staffers. They have tried to compensate for the lack of senior people by bringing in external speakers, often via Zoom, and by having internal seminars, but this is unlikely to be enough: outsiders cannot provide sufficient mentoring. The situation calls for careful succession planning to balance costs and benefits in a workforce transition.

## EFFECTIVENESS OF DISSEMINATION EFFORTS

CSD is getting its message out to its stakeholder communities. Between January 2018 and May 2024, the number of subscribers to its products grew, sometimes substantially. For example, the increase in the following subscribers was

- Draft publications: 31 percent
- Federal Information Processing Standards: 21 percent
- Federal Information Systems Management Act News: 192 percent
- Risk management–related publications: 190 percent
- NIST Cybersecurity Events: 115 percent
- NIST Internal Reports: 24 percent
- Special publications: 15 percent

Copyright National Academy of Sciences. All rights reserved.

Computer Security Resource Center use has seen the following growth between 2018 and 2023:

- Total sessions: 133 percent
- Total users: 193 percent
- Users per day: 193 percent
- Page views: 112 percent
- Publication details (page views): 90 percent
- Cryptographic Module Validation Program validations (certificate page views): 190 percent

CSD has published 93 new final reports since January 1, 2018. CSD has hosted 16 conferences and workshops since 2018, including 6 on PQC, 4 on LWC, 3 on threshold cryptography, and 2 on modes. They have ongoing seminars: the Crypto Reading Club, the PQC Seminar Series, and Privacy and Auditability. In addition, CSD participates in the Internet Engineering Task Force; the International Organization for Standardization and the International Electrotechnical Commission Subcommittee 27 on Information Security, Cybersecurity, and Privacy Protection; the Trusted Computing Group; and the Bluetooth Special Interest Group.

Also since 2018, CSD staff have authored

- 33 conference papers,
- 23 journal articles,
- 18 book chapters, and
- 23 preprint papers.

ITL groups state their accomplishments in terms of outputs (e.g., number of papers, number of patents, number of meetings convened) rather than in terms of outcomes (e.g., impacts on U.S. commerce, dollar size of the ecosystems they support, or number of times a standardized algorithm is used per minute). Outputs are easier to measure than outcomes, but they are not impressive to appropriators. ITL would be well served to quantify and describe its support of U.S. industry, and to collect and tell industry use case stories when dealing with legislative staff. Similarly, concerning ITL’s massive support of federal agencies, it would be advantageous to collect and tell use case stories rather than simply recite the number of publications produced.

As an example of measuring outcomes, NIST maintains a webpage titled Outputs and Outcomes of NIST Laboratory Research (created on July 20, 2009, and last updated on June 2, 2021, so this is only an example). It lists the economic impact of selected NIST research efforts. ITL has four listings on this webpage:

- 1995: Interoperability standards for Integrated Services Digital Network leading to lower transaction costs: social (internal) rate of return of 156 percent.
- 1995: Acceptance test methods for software conformance leading to lower transaction costs: social (internal) rate of return of 41 percent.
- 2001: Standard conformance test methods and services for data encryption standards: social (internal) rate of return of 267–272 percent; a benefit–cost ratio ranging from 58 to 145; and net present value ranging from $345 million to $1.2 billion.
- 2001: Generic technology reference models for role-based access control enabling new markets and increasing research and development efficiency: social (internal) rate of return of 44 percent; a benefit–cost ratio of 109; and net present value of $292 million. (NIST 2021)

**Recommendation 5-4: The Computer Security Division should explore and develop metrics that measure the impact and outcomes resulting from its work rather than simply counting outputs.**

Copyright National Academy of Sciences. All rights reserved.

## REFERENCE

NIST (National Institute of Standards and Technology). 2021. *Outputs and Outcomes of NIST Laboratory Research.* https://www.nist.gov/director/outputs-and-outcomes-nist-laboratory-research.

Copyright National Academy of Sciences. All rights reserved.

# 6
# Information Technology Laboratory's Responses to the Recommendations of Previous Assessment Reports

This chapter provides the Information Technology Laboratory's (ITL's) responses to recommendations made in the previous assessments of the divisions in this report by the National Academies of Sciences, Engineering, and Medicine in fiscal year (FY) 2018 (NASEM 2018), and some recommendations from the FY 2021 assessment (NASEM 2021). The sections below include observations on specific recommendations from 2018 that were addressed to the offices and divisions.

## 2018 REPORT

### Staffing and Recruitment

**Recommendation:** The [Applied Computational and Mathematics Division] (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.

> *ITL response:* We have greatly *increased* our pool of participants. During the period October 2022–December 2023, we
>
> - Hosted 9 NIST/NRC postdoctoral associates
> - Engaged with 12 postdoctoral or senior researchers through the PREP program, contracts, or grants
> - Supported 2 technicians via contracts
> - Supported 13 graduate research assistants through the PREP, the NIST foreign guest researcher program, and the NSF Math Science Internship program
> - Supported the part time work of 8 faculty members
> - Formally engaged with many others as unpaid guest researchers
> - Informally engaged with many additional collaborators worldwide.

**Recommendation:** The [Computer Security Division] (CSD) should consider adding staff to the Lightweight Cryptography project.

> *ITL response:* Complete: <3 new staff members were added> to the Lightweight Cryptography project.

**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.

Copyright National Academy of Sciences. All rights reserved.

> *ITL response:* Complete: <A staff member> was added to Combinatorial Methods team.

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

> *ITL response:* Complete: CVE backlog issue from that period addressed. Current and new CVE issue being addressed with new short-term resource allocations.

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

> *ITL response:* Complete and Ongoing: New mid-career staff added in each group.

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

> *ITL response:* ITL continues to expand our use of the PREP program—since the last panel meeting ITL has employed 42 new PREP staff, including international students attending U.S. universities.

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

> *ITL response:* According to NIST HR DATA, ITL's candidate pools between May 2021–Feb 2024 for all pay plans (ZA, ZS, ZP) was 48% minority, 32% nonminority, 20% omitted. During the same period ITL's candidate pools were 35% female, 47% male, 19% omitted. During this period the percent of total staff increased by 4% for females, 3% for minorities, and our hires in this period were 50% females. ITL leadership emphasizes the importance of seeking diverse candidate pools—and the use of tools such as LinkedIn recruiter. The staff led ITL Diversity Committee is implementing its strategic plan in coordination with management. ITL proposed tools that NIST now uses to ensure language of job openings is not biased. All Group Leaders are being interviewed about recruiting and retention to share best practices and lessons learned.

## Technical Planning

**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.

> *ITL Response:* An Applied and Computational Mathematics Division Capability Plan was developed in 2019 which has the requested features.
>
> Table of Contents
> 1 Introduction: The Division and Its
> Operations
> Customers
> Approach
> Relation to Internal Customers
> Relation to External Customers
> Project Selection

Copyright National Academy of Sciences. All rights reserved.

2 Capabilities Needed for the Future
2.1 Math and Comp Foundations of Adv Metrology
2.2 Future Computing Technologies
2.3 Mathematical Knowledge Management
3 Meta Issues
3.1 Coping with a Wave of Retirements
3.2 Ensuring Diversity in the Workforce
3.3 Developing Competencies in New Areas
3.4 Developing the NIST Customer Base
3.5 Physical Location of NIST Staff
4 Staffing Trends and Needs

Technical Areas Identified for Growth

- Quantum-based measurements
- Bioscience*
- Measurement science for information technology
- Data, machine learning, and AI*
- Dynamic metrology
- Imaging systems as metrological devices
- Multiscale material modeling
- Metrology for modeling and simulation
- Quantum information theory*
- Quantum architectures, benchmarking, and testing*
- Quantum communication systems and components*
- Neuromorphic computing
- Mathematical knowledge management

While there has been activity in all these areas, those asterisked have seen the biggest increases.

## Conferences and Publications

**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.

> *ITL Response:* Conference attendance is determined by Division management who assess the return on investment with respect to advancing the NIST mission in deciding when to send staff to conferences. Presenting research results is the highest priority, but the importance of staff development by engaging with national and international collaborators on the latest research, is another important consideration. ITL publishes in both conference proceedings and scholarly journals—depending on the type of research and the target audience.

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

> *ITL Response:* Individual staff members have continued to engage in self-study to increase knowledge, skills, and abilities in this area. Machine learning techniques and workflows is one example. Research software engineering is an area in which we would like to grow, and we have had some recent contract support in this area, but budgetary and recruiting considerations make expansion a challenge.

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

Copyright National Academy of Sciences. All rights reserved.

> *ITL Response: Complete:* Access control shifted to tech transfer opportunities and newer technologies.

**Recommendation:** The CSD should take steps to publicize the Lightweight Cryptography [LWC] program among potential users of the resulting algorithms—particularly Internet of Things [IOT] vendors and customers.

> *ITL Response:* Complete and Ongoing: LWC project continues as final algorithm selection is finished. Direct outreach includes to the IOT program and potential affected communities (i.e., space, automotive, etc.).

**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.

> *ITL Response:* Complete and Ongoing: Crosses several avenues from annual reviews of use of posted references, completion of impact studies, reviews of industry access to CSD data and [Standards Developing Organization] adoption.

**Recommendation:** The CSD, in partnership with the [Applied Cybersecurity Division] ACD, should investigate and, if possible, develop and disseminate metrics for privacy.

> *ITL Response:*
>
> - CSD: Completion of Privacy Controls in SP 800-53 and Privacy Assessment Methods in SP 800-53A.
> - ACD: The Privacy Engineering Program established the Collaborative Research Cycle to benchmark data de-identification techniques and develop metrics.

**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 [National Cybersecurity Center of Excellence] 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.

> *ITL Response:* The recommendation was elevated to ITL for crisis communication preparation, including tabletops, for all NIST cybersecurity publications.

**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.

> *ITL Response:* Recommendation not implemented. The NCCoE reviewed the recommendation and considered the value that adversarial review (i.e., red-teaming) would bring to a project solution. The value of NCCoE technical projects is the architecture with the products involved to provide examples that demonstrate possible solutions. An adversarial red-team type of review would test the products within a build rather than the architecture. While this could provide value to a specific lab instance, it would be detrimental to the NCCoE’s relationship with its collaborators. It would also only be relevant for organizations using the exact setup and products indicated in the NCCoE project. In addition, NCCoE

Copyright National Academy of Sciences. All rights reserved.

builds only represent the part of an architecture that is relevant to the security challenge in question. It is likely that organizations will have additional controls in place that would not be tested in this type of red team activity.

**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.

*ITL Response:* NCCoE sought to participate with universities through 1. Capstones for students to research a topic of interest to the NCCoE and 2. Expansion of student work-based learning opportunities that leverage both NIST and MITRE intern programs. New NCCoE leadership is exploring how to increase stakeholder engagement (including academia) on NCCoE projects, including to define cybersecurity challenges and increase use of NCCoE outputs. NCCoE hopes to find ways to leverage the academic community for new project ideas, as well as technical participation on 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.

*ITL Response:* The NCCoE tracks several metrics associated with impact, including publication downloads, event attendance, COI subscribers, CRADA numbers, as well as qualitative discussions with the community on the use of NCCoE outputs.

New leadership has defined the need to measure impact of the NCCoE's work as a top priority. Tiger teams have been recently stood up representing leadership and engineers across NIST and MITRE to identify additional metrics to define impact, set up a process for project reviews, as well as find ways to increase communication on successes across the NCCoE and with the public.

## 2021 REPORT

### Technical Expertise of the Staff and Adequacy of Staffing

**Recommendation:** ITL should apply an aggressive, imaginative focus on hiring to replace retiring staff, to address important growth areas such as artificial intelligence, machine learning, and data science, and to fill specific gaps in the divisions. This effort should aspire to diversity targets.

*ITL Response:* ITL has hired 17 new staff in [artificial intelligence], [machine learning], and data science across all our divisions. When recruiting we ignite candidates' imaginations regarding how they can work in ITL to solve national and international problems—e.g., the safe and trustworthy use of Artificial Intelligence, cybersecurity, privacy, quantum computing and networking and much more. We receive large number of candidates for these job openings.

**Recommendation:** ITL should plan and implement effective ways to recruit and retain a diverse workforce to ensure the appropriate staffing in areas of significant interest to national welfare and security, and to address severe competition from industry in areas such as artificial intelligence, cybersecurity, and the [IOT].

*ITL Response:* ITL's diversity committee developed a strategic plan with 4 main objectives, 26 strategies, and associated success measures to improve recruiting and retention of a diverse

Copyright National Academy of Sciences. All rights reserved.

An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024

> workforce. ITL implemented a Speaker's Bureau and reached out to minority serving universities to offer ITL experts to give talks about their work and opportunities at NIST. ITL recruits staff who are motivated to make a difference in the world through our research, standards, measurements, testing, and guidance in critical areas such as [artificial intelligence], cybersecurity, privacy, quantum, biometrics, software testing, and others. ITL also uses all HR capabilities to retain staff, such as retention bonuses.

**Recommendation:** ITL should establish exchange programs with relevant government laboratories, academic institutions, and industry consortia to stimulate new ideas and problem areas, enhance competencies, and facilitate collaboration.

> *ITL Response:* ITL actively pursues staff exchange—with researchers coming to NIST as well as NIST staff going to other organizations. Since our last panel meeting ITL has had 59 new staff exchanges with universities and government agencies both in the U.S. and around the world.

### Adequacy of Facilities and Equipment

**Recommendation:** ITL should take steps to ensure adequate resources, especially computing to support AI/ML and data science at sufficient scale.

> *ITL Response:* ITL provided 3 computing experts to the NIST Research Computing Infrastructure Task Force. With ITL leadership the task force succeeded in getting approval for a complete renovation and update of NIST's local computing resources as well as formal plans for access to external HPC resources. The Task Force developed a detailed and compelling vision for how access to adequate computing resources is critical to NIST's future. This investment will benefit ITL, and all NIST researchers, through an effective, scalable, shared approach to computing infrastructure.

**Recommendation.** To get access to the most modern resources, ITL should seek collaborations with other organizations in the public and private sectors, including other Government agencies. To achieve collaborative access, the ITL should examine its potential contributions to partnerships.

> *ITL Response:* Since our last [National Academies] review, ITL has established 469 new collaborations to expand access to new methodologies and approaches, and access modern resources. These collaborations are critical to all the work carried out in ITL—nearly all ITL staff have external collaborators for their work.

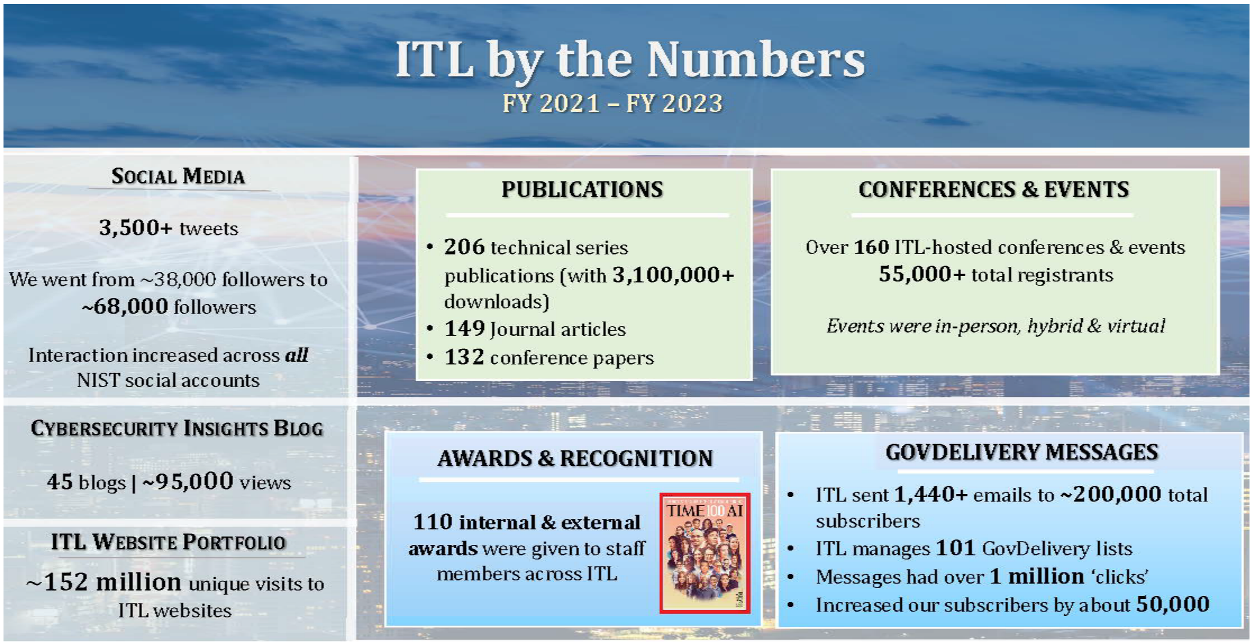
### Effectiveness of the Dissemination of Outputs

**Recommendation:** ITL should broaden its impact to non-technical stakeholders, policy makers, and the public.

> *ITL Response:* ITL communicates its value through the use of the internet, including social media (e.g., @NISTCyber) and high visibility events with Congress, the White House, workshops, and conferences. In addition, ITL actively supports Take Your Kids to Work Day to encourage youth participation in STEM. More information on the dissemination of outputs and technology transfer for the three divisions under review is available in the read-ahead material and on the ITL NASEM supplemental webpage and in the infographic below [Figure 6-1].

Copyright National Academy of Sciences. All rights reserved.

An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024



**ITL by the Numbers**

**FY 2021 – FY 2023**

**SOCIAL MEDIA**

**3,500+** tweets

We went from ~38,000 followers to **~68,000** followers

Interaction increased across ***all*** NIST social accounts

**PUBLICATIONS**

- **206** technical series publications (with **3,100,000+** downloads)
- **149** Journal articles
- **132** conference papers

**CONFERENCES & EVENTS**

Over **160** ITL-hosted conferences & events

**55,000+** total registrants

*Events were in-person, hybrid & virtual*

**CYBERSECURITY INSIGHTS BLOG**

**45** blogs | **~95,000** views

**ITL WEBSITE PORTFOLIO**

~**152 million** unique visits to ITL websites

**AWARDS & RECOGNITION**

**110 internal & external awards** were given to staff members across ITL

**GOVDELIVERY MESSAGES**

- ITL sent **1,440+** emails to **~200,000** total subscribers
- ITL manages **101** GovDelivery lists
- Messages had over **1 million** 'clicks'
- Increased our subscribers by about **50,000**

**FIGURE 6-1** Dissemination of the Information Technology Laboratory's (ITL's) outputs.
SOURCE: Courtesy of NIST Information Technology Laboratory.

## REFERENCES

NASEM (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*. The National Academies Press. https://doi.org/10.17226/25283.

NASEM. 2021. *An Assessment of Selected Divisions of the Information Technology Laboratory at the National Institute of Standards and Technology: Fiscal Year 2021*. The National Academies Press. https://doi.org/10.17226/26354.

Copyright National Academy of Sciences. All rights reserved.

# 7
# Overarching Themes, Key Recommendations, and Chapter Recommendations

## OVERARCHING THEMES AND KEY RECOMMENDATIONS

### Strategic Direction and Strategic Planning

The panel noted that, despite impressive outcomes, ITL appears to need a more structured strategic plan, with new projects appearing to be primarily driven by legislation and executive orders. Concerns were raised about future staffing levels owing to potential retirements, which could spread available resources too thin and reduce ITL's ability to deliver broader and more impactful outcomes. Although some strategic vision was evident, it needs clearer and more systematic development and efficient collaboration both within and outside NIST. Developing a well-structured strategic plan would holistically align ITL's diverse projects with current and future trends, external demands, and emerging topics, helping to consolidate efforts and enable the efficient use of resources.

The panel also found that criteria for defining, prioritizing, and evaluating projects were sometimes not sufficiently clear, and ITL's overwhelming project demands and budget constraints limit its capacity for in-depth project work. Improved coordination, mentoring, and cross-group collaboration are needed to align projects with ITL's mission and optimize resource use.

**Key Recommendation 1: The Information Technology Laboratory should create a structured strategic plan based on its overarching vision to concentrate its efforts and resources on the most critical areas of work. This will help avoid initiation of projects that are misaligned with the division's strategic goals and prevent the dilution of resources, ensuring greater impact.**

### Metrics and Stakeholder Relevance

The panel observed that ITL currently measures its accomplishments based on outputs such as the number of papers, patents, and meetings, rather than outcomes such as impacts on U.S. commerce, the economic scale of supported ecosystems, or the frequency of algorithm usage. Such outputs are easier to quantify but may not impress appropriators. ITL would benefit from focusing on and communicating the tangible impacts on U.S. industry and sharing industry use case stories with legislative staff. Similarly, for ITL's extensive support of federal agencies, collecting and sharing use case stories would be more effective in communicating impacts than merely reporting the number of publications.

The panel strongly believes that the division's work appeals to a broader audience beyond its typical stakeholders. While ITL engages with NIST's Public Affairs Office, it is unclear whether current communication channels adequately highlight ITL's work to external stakeholders. Researchers engage with the academic community and the Department of Commerce, but a clear strategy for broader external communication could be impactful. Key questions to address include the following: Which additional communities should ITL's work reach (e.g., Congress, industry, education, or citizens)? What positive

Copyright National Academy of Sciences. All rights reserved.

outcomes could arise from broader engagement (e.g., increased funding or better access to resources)? What are the most effective communication channels (e.g., events, videos, textual content)? What is ITL's web presence strategy, and what resources are needed to optimize communication outcomes?

ITL's work appeals to a broader audience, but current communication channels may not effectively reach external stakeholders. The panel suggests improving visibility to various communities (e.g., Congress, industry, academia) and enhancing communication strategies, including web presence. Additionally, while dissemination metrics focus on reach, there is a need for metrics that measure and communicate impact to stakeholders and appropriators and that these be included in the strategic plan.

ITL needs to develop metrics that better assess and communicate the impact of its projects to stakeholders and appropriators. Considering constraints on surveying stakeholders, ITL might explore alternative metrics, such as tracking external contributions to ITL documents or reported issues by adopters. Ideas from the open-source community, like those outlined in the Linux Foundation's "Measuring Your Open Source Program's Success" could be useful.[1] Additionally, measuring the percentage of repeat collaborating companies could indicate industry value, with different implications for small start-ups versus large technology firms. Years ago, NIST did contract some NIST impact studies (NIST 2023). These studies might be a useful template for ITL to measure impact.

> **Key Recommendation 2: The Information Technology Laboratory (ITL) should develop impact metrics to be applied uniformly across all of its work. Metrics should, whenever possible, include both the economic benefits for adopters and measurable reductions in risk. These metrics should illustrate the impacts and outcomes of ITL's work rather than simply providing outputs. Plans for improved communication with ITL's current and potential stakeholders should be included in the strategic plan.**

## Artificial Intelligence

The panel believes that artificial intelligence (AI) will significantly impact ITL's work, with potential opportunities including the use of large language models for scientific and mathematical discovery and enhancing these models. The panel recommends that ITL develop a more ambitious AI strategy focused on critical infrastructures, tools, and methods, and identify key areas for national and international leadership.

Recent advancements in foundational AI and its applications have been revolutionary, and AI is expected to affect nearly all aspects of life and commerce in the coming years. However, its impact on computer security remains uncertain. AI can be used by both attackers and defenders, and the introduction of new AI-driven products and services will bring risks that are not yet fully understood. Additionally, there are growing privacy concerns surrounding the data used to train AI systems. All of this suggests tremendous technological opportunities for ITL.

The panel emphasizes that for ITL to remain effective over the next decade, it must invest in AI staffing, equipment, and expertise. While hiring permanent staff is a long-term solution, establishing a contractor-based or visiting researcher program could be a practical short-term arrangement to enable more agile knowledge transfer. This approach would allow the division to swiftly explore how contemporary AI techniques, such as large language models, can be integrated into existing research workflows.

Cutting-edge research, model training, and AI inference require substantial investment in hardware, data, software, operational resources (such as power), and staff. Building these capabilities will be costly, and attracting top talent will depend on ensuring adequate facilities.

[1] See the Linux Foundation's Open Source Guide "Measuring Your Open Source Program's Success" at https://www.linuxfoundation.org/resources/open-source-guides/measuring-your-open-source-program-success, accessed August 21, 2024.

Copyright National Academy of Sciences. All rights reserved.

**Key Recommendation 3: The Information Technology Laboratory should enhance its artificial intelligence (AI) expertise to continue being able to have significant impacts in this area. In the long term, this will require adding AI researchers and engineers, either by hiring new talent or by upskilling current staff, or a combination of both. In addition to building a permanent team, the division can create a contractor or visiting researcher program to facilitate flexible knowledge transfer in AI. Such initiatives could also help identify potential candidates for future hiring.**

## CHAPTER 3: APPLIED CYBERSECURITY DIVISION

**Recommendation 3-1: Existing and new Applied Cybersecurity Division projects should include the study of the security, privacy, and responsible uses of artificial intelligence (AI), including the security and privacy characteristics of AI systems.**

**Recommendation 3-2: The Applied Cybersecurity Division (ACD) should focus on the development of new, specialized cybersecurity guidance for single proprietor or partnership businesses with only a few employees. It should partner with the Small Business Association to develop training materials such as videos and checklists and support regional outreach to enable ACD to have a broader impact within the limited resources available to the program.**

**Recommendation 3-3: The Applied Cybersecurity Division should conduct a study of the target audiences for its Cybersecurity Framework Profiles to determine if they are being used to full effect, and to determine if their content and format are appropriate for the intended audiences. The Statistical Engineering Division should be consulted on this. Future profiles and the allocation of resources to support their development should be informed by this study.**

**Recommendation 3-4: The Applied Cybersecurity Division should supplement its work on digital identities with a study of the implications and remediation of a large-scale cyberattack on modern identity systems, such as what might arise from vulnerabilities in widely used desktop or mobile operating systems.**

**Recommendation 3-5: The Applied Cybersecurity Division (ACD) should explore innovative approaches to staff augmentation and retention. ACD should also develop programs to engage senior volunteer cybersecurity research and engineering talent to serve the nation through its programs and activities.**

**Recommendation 3-6: The Applied Cybersecurity Division should develop impact metrics for individual projects and apply them uniformly. Metrics should include economic benefits for adopters and quantification of risk reduction, where possible. Useful ideas may be found, for example, through the open-source community and the Linux Foundation.**

**Recommendation 3-7: The Applied Cybersecurity Division (ACD) should develop and share a strategic vision for how projects are selected and managed in ACD to balance the demands on the division with the available resources and prevent the loss of value and impact from being overstretched.**

Copyright National Academy of Sciences. All rights reserved.

## CHAPTER 4: APPLIED AND COMPUTATIONAL MATHEMATICS DIVISION

**Recommendation 4-1: The Applied and Computational Mathematics Division should develop a strategic plan, derived from its strategic vision, to focus its efforts and resources on what have been determined to be the most important lines of work and to prevent the establishment of projects that are not aligned with the strategic vision and that would diffuse the division's resources and reduce its impact.**

**Recommendation 4-2: The Applied and Computational Mathematics Division should develop a strategic plan that reflects an integrated vision of the impact of artificial intelligence (AI) on the division, both the short and long term. This plan should address critical questions such as the following:**

- **a. How can AI support and improve productivity for mathematical modeling?**
- **b. Which infrastructures, tools, and methods are critical within this context?**
- **c. What are the key strategic areas of involvement and opportunities for national and international leadership within the AI space?**

**Recommendation 4-3: The Applied and Computational Mathematics Division should expand the artificial intelligence (AI) expertise available to it. In the long term, it should add AI researchers and engineers. This can be accomplished through new hires, upskilling existing staff, or both. Until it can bring on permanent staff in this area, the division should establish a contractor-based or visiting researcher program to support a more agile knowledge transfer in this domain. These programs might help identify candidates for hiring.**

**Recommendation 4-4: The Applied and Computational Mathematics Division should designate rooms that its staff can use for remote meetings and remote and in-person conferences with other researchers without the need to schedule them in advance.**

**Recommendation 4-5: The Applied and Computational Mathematics Division (ACMD) should maintain the Handbook of Mathematical Functions. ACMD should consider whether the division wants to develop new reference materials for the mathematical community.**

**Recommendation 4-6: The Applied and Computational Mathematics Division (ACMD) should develop a strategy for the improved communication of its work to stakeholders. ACMD should also develop additional metrics to better illustrate the impacts of its ongoing work.**

## CHAPTER 5: COMPUTER SECURITY DIVISION

**Recommendation 5-1: To increase security, automate as much of the workload as possible, and reduce operating costs, the Computer Security Division should migrate access to the National Vulnerability Database to an application programming interface as rapidly as possible.**

**Recommendation 5-2: The Computer Security Division (CSD) should engage in a strategic planning process to intentionally choose projects that align with its mission and make the best use of the division's extremely limited resources. This plan should also consider when projects have been successful and what projects ought to be retired to free up resources for new work.**

Copyright National Academy of Sciences. All rights reserved.

**This plan should be clearly communicated to all CSD staff so that they understand exactly how their work fits into the broader divisional mission.**

**Recommendation 5-3: To free up staff and financial resources for new work, the Computer Security Division should hand off developed technologies to others such as contractors to operate. This will allow researchers to focus on what they are good at and put operations in the hands of those who are skilled at it.**

**Recommendation 5-4: The Computer Security Division should explore and develop metrics that measure the impact and outcomes resulting from its work rather than simply counting outputs.**

## REFERENCE

NIST (National Institute of Standards and Technology). 2023. “Summary of NIST Impact Study Results.” Updated August 23. https://www.nist.gov/tpo/summary-nist-impact-study-results.

Copyright National Academy of Sciences. All rights reserved.

# Appendixes

Copyright National Academy of Sciences. All rights reserved.

Copyright National Academy of Sciences. All rights reserved.

# A
# Acronyms and Abbreviations

| | |
|---|---|
| ACD | Applied Cybersecurity Division |
| ACMD | Applied and Computational Mathematics Division |
| AES | Advanced Encryption Standard |
| AI | artificial intelligence |
| API | application programming interface |
| CSD | Computer Security Division |
| FIPS | Federal Information Processing Standards |
| FTE | full-time equivalent |
| FY | fiscal year |
| IEEE | Institute of Electrical and Electronics Engineers |
| IoT | Internet of Things |
| ISO | International Organization for Standardization |
| IT | information technology |
| ITL | Information Technology Laboratory |
| LWC | lightweight cryptography |
| NCCoE | National Cybersecurity Center of Excellence |
| NIST | National Institute of Standards and Technology |
| NVD | National Vulnerability Database |
| OOMMF | Object Oriented MicroMagnetic Framework |
| PQC | post-quantum cryptography |
| QuICS | Joint Center for Quantum Information and Computer Science |
| SBA | Small Business Administration |
| SHA | Secure Hash Algorithm |
| STRS | scientific and technical research services |
| VCAT | Visiting Committee on Advanced Technology |

Copyright National Academy of Sciences. All rights reserved.

# B
# Panel Member Biographical Information

KWANG-CHENG CHEN, *Chair*, has been a professor in the Department of Electrical Engineering, University of South Florida, and on the cybersecurity faculty with Cyber Florida after his career with the IBM T.J. Watson Research Center, HP Labs, COMSAT Corporation, and National Taiwan University and National Tsing Hua University in Taiwan. Dr. Chen's patented technology has been adopted in Bluetooth, IEEE 802.11 wireless LANs (Wi-Fi), 4G and LTE-A, and 5G mobile communications. His start-up company delivered the world's first on-chip Advanced Encryption Standard in wireless integrated circuits, and the first low-power broadband wireless solution for smartphones. Dr. Chen is an Institute of Electrical and Electronics Engineers (IEEE) fellow and a recipient of the 2014 IEEE Jack Neubauer Memorial Award, 2011 IEEE Communications Society Wireless Communications Technical Committee Recognition Award, and many paper awards for his IEEE journal and conference papers. Dr. Chen served the National Academies of Sciences, Engineering, and Medicine's Panel on Review of the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) in 2018.

GAIL-JOON AHN is a professor of computer science and engineering in the School of Computing and Augmented Intelligence and the founding director of the Center for Cybersecurity and Trusted Foundations at Arizona State University. Dr. Ahn's principal research and teaching interests are in the areas of information and systems security. His research has been supported by the National Science Foundation (NSF), National Security Agency, Department of Defense (DoD), Department of Energy (DOE), Office of Naval Research, Cisco, GoDaddy, Bank of America, Hewlett Packard, Microsoft, Samsung, PayPal, and Robert Wood Johnson Foundation. Dr. Ahn is currently the information director of the Association for Computing Machinery (ACM) Special Interest Group on Security, Audit, and Control and has served as the associate editor-in-chief of *IEEE Transactions on Dependable and Secure Computing*, on the editorial board of *Computers and Security*, and as the associate editor of *ACM Transactions on Information and System Security*. He is a recipient of DOE's Early Career Principal Investigator Award and has published more than 250 articles in reputed journals and conferences, accumulating more than 17,000 citations. He is also the recipient of the Educator of the Year Award given by the Federal Information Systems Security Educators Association in 2005. Dr. Ahn is a fellow of IEEE and holds 10 U.S. patents in the field of computer science and engineering.

JANDRIA S. ALEXANDER is a vice president at Booz Allen Hamilton, where she leads technology and mission solutions for government clients. Ms. Alexander leads the delivery of cybersecurity, software, data science, cyber-physical systems, and research and development (R&D). She is a subject-matter expert on cybersecurity, resilient platforms, operational technology, and multidomain mission systems, with more than 20 years in the field. A nationally recognized cybersecurity expert, Ms. Alexander has participated in National Academies' studies related to cybersecurity research and new aviation technologies. In 2014, she was appointed by former Virginia Governor Terry McAuliffe to serve on the bipartisan Virginia Cyber Security Commission to expand the state's economic footprint in cyber technology and protect critical infrastructure from cyber threats. She led the effort's unmanned systems cybersecurity industry, government, and academia consortium. Over the length of her career, Ms. Alexander has provided cybersecurity and digital transformation leadership, market strategy, and solution

Copyright National Academy of Sciences. All rights reserved.

development for DoD and the intelligence community as well as many civil and commercial organizations. Before joining Booz Allen in 2017, she was a cybersecurity leader in engineering and technology at a federally funded research and development corporation. She served as the chair of the American Institute of Aeronautics and Astronautics (AIAA) Diversity and Inclusion Working Group from 2017–2021, a member of the Defense Conference Board, and an advisor on the Adoption of Artificial Intelligence (AI) for AIAA. She has a BS in computer science from Brandeis University and an MS in technology management from American University.

STEVEN M. BELLOVIN is the Percy K. and Vidal L.W. Hudson Professor of Computer Science at Columbia University, a member of the Cybersecurity and Privacy Center of the university's Data Science Institute, and an affiliate faculty member at Columbia Law School. Dr. Bellowvin does research on security and privacy and on related public policy issues. He received a BA from Columbia University and an MS and a PhD in computer science from the University of North Carolina at Chapel Hill. Dr. Bellovin has served as the chief technologist of the Federal Trade Commission and as the technology scholar at the Privacy and Civil Liberties Oversight Board. He is a member of the National Academy of Engineering (NAE) and has served on the Computer Science and Telecommunications Board of the National Academies. In the past, he has been a member of the Department of Homeland Security's Science and Technology Advisory Committee and the Technical Guidelines Development Committee of the Election Assistance Commission.

THOMAS A. BERSON is the founder of Anagram Laboratories, an information security consultancy. He is also the cybersecurity advisor to the chief executive officer and the Board of Directors at Salesforce. Prior to Anagram, Dr. Berson co-founded and was the vice president of research at Sytek, acquired by Hughes Network Systems. He earlier worked at IBM Research, Ford Aerospace, and Xerox PARC. He has experience in the design, implementation, and evaluation of cryptosystems, including algorithms and key distribution protocols. While at Sytek, Dr. Berson developed end-to-end encryption, challenge and response authentication, and high-assurance cross-domain products. At Salesforce, he wrote the cloud security policy and mentors executives responsible for establishing, operating, and governing trust worldwide. Dr. Berson is a member of NAE and a fellow of the International Association for Cryptologic Research (IACR). He was an editor of the *Journal of Cryptology* and served as the chair of the IEEE Technical Committee on Security and Privacy. Dr. Berson earned his BS in physics from the State University of New York and his PhD in computer science from the University of London. He was a visiting fellow in mathematics at Clair Hall, Cambridge. He has been a member of relevant past National Academies' committees, including the Committee to Review DOD C4I Plans and Programs, the Committee on Offensive Information Warfare, and the Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of National Academies Work. He is currently a member of the National Academies' Forum on Cyber Resilience.

CHARLES BLAUNER is an internationally recognized expert independent advisor on cyber resiliency, information security risk management, and data privacy. He is the president of Cyber Aegis, a boutique cyber risk management consultancy. Mr. Blauner is also an operating partner and the chief information security officer (CISO) in residence at Team8 Ventures, an operating advisor at Crosspoint Capital, a venture advisor at the Cyber Mentor Fund, and an executive in residence at the Partnership Fund for New York City's FinTech Innovation Lab. Previously, he had a distinguished career working on information and cyber security for more than 30 years, in financial services for 25 years, including being the CISO at JP Morgan and Deutsche Bank, and most recently the global head of information security at Citi. During this time, Mr. Blauner held numerous industry leadership roles, including the chair of the Financial Services Sector Coordinating Council, founding director of the Financial Services Information Sharing and Analysis Center, and chair of the OpenGroup's Security Program. He has worked closely with banking regulators around the world (Office of the Comptroller of the Currency, Federal Reserve Board, Bank of England, Monetary Authority of Singapore, and Hong Kong Monetary Authority) to help reduce

Copyright National Academy of Sciences. All rights reserved.

the risk posed by cyber threats to the financial sector at large. Mr. Blauner is a regular conference speaker and has had the honor of appearing in front of U.S. House and Senate committees. In 2015, he was recognized by his peers, winning the Wasserman Award, which recognizes outstanding career achievement and contribution to the information systems audit, control, security, risk management, and/or governance professions. Mr. Blauner has an MS in computer science from the University of Southern California and a BS in computer science from Rensselaer Polytechnic Institute.

RUSSEL E. CAFLISCH is currently the director of the Courant Institute of Mathematical Sciences at New York University (NYU). Prior to this position, he was the director of the Institute for Pure and Applied Mathematics at the University of California, Los Angeles (UCLA), 2008–2017, and he held faculty positions at Stanford University and UCLA. Dr. Caflisch is an applied mathematician whose research is on analysis and numerical methods for physical sciences. He is known for analysis of the fluid dynamic limit in kinetic theory and of vortex sheets in incompressible flow, mathematical modeling of epitaxial growth, and development of Monte Carlo methods for kinetic theory and finance. Dr. Caflisch is a member of the National Academy of Sciences (NAS) and a fellow of the American Academy of Arts and Sciences (AAA&S). He graduated from Michigan State University with a BS in mathematics in 1975 and received his PhD in mathematics in 1978 at the Courant Institute, NYU.

KELLY CAINE is a professor in the Human-Centered Computing Division of the School of Computing at Clemson University. Dr. Caine is the founder and co-director of the Humans and Technology Lab (www.hatlab.org), where she leads research in human factors, cybersecurity, human-centered computing, privacy, usable security, and human–computer interaction. Her work in these areas has been continuously funded by agencies such as NSF for more than a decade. She is the co-author of *Understanding Your Users: A Practical Guide to User Research* (2015) and has published more than 100 peer-reviewed papers in venues ranging from ACM CHI to the *Journal of the American Medical Informatics Association*. Dr. Caine and her students have received awards for their collaborative research from NAE, the Institute of Medicine, the American Public Health Association, and the Human Factors and Ergonomics Society. She is key faculty in Clemson's Cybersecurity Center, an associate in the Human Factors Institute, and a member of the Human Factors and Ergonomics Society. Prior to joining Clemson, Dr. Caine was a principal research scientist in the School of Computing at Indiana University's Center for Applied Cybersecurity Research, and a UX researcher at Google. She holds degrees from the University of South Carolina (BA) and the Georgia Institute of Technology (MS and PhD).

RICHARD CHOW is a university research director and scientist in the University Research and Collaboration office within Intel Labs. Dr. Chow guides several of Intel's academic research centers in the areas of security, networking, autonomous systems, and machine learning. In the past, he has held positions as a research scientist at PARC, a research scientist at Samsung Electronics R&D, and a security architect at Yahoo and Motorola. Dr. Chow has more than 20 U.S. patents and patent applications and more than 30 peer-reviewed journals, conference papers, and book chapters. He was awarded runner-up for the 2010 PET Award for Outstanding Research in Privacy Enhancing Technologies. Dr. Chow has a PhD in mathematics from UCLA and a BA in mathematics from the University of Pennsylvania.

PAUL ENGLAND is an independent consultant. Previously, he was a distinguished engineer at Microsoft Research working on computer security. Dr. England is best known for foundational work in trusted and confidential computing. This includes various hardware roots-of-trust, such as the Trusted Platform Module, and the secure-enclave technologies that are now implemented in most mainstream microprocessors and supported in most mainstream operating systems. Dr. England has advised governments and regulators on many aspects of cybersecurity and policy. He was elected to NAE in 2019 for these contributions. Dr. England has a PhD in condensed matter physics from Imperial College, London.

Copyright National Academy of Sciences. All rights reserved.

ANDRÉ FREITAS is an associate professor (senior lecturer) at the Department of Computer Science at the University of Manchester (UK), an AI Group leader at the Cancer Research UK Manchester Institute and a Research Group leader at the Idiap Research Institute (Switzerland). He leads the Neuro-Symbolic AI Group. His main research interests are on enabling the development of AI/Natural Language Processing (NLP) methods to support complex and controlled expert-level inference, with a particular emphasis on supporting scientific discovery. He is an active contributor to the main conferences and journals in AI/NLP, including the Association for the Advancement of Artificial Intelligence (AAAI), Neural Information Processing Systems, Association for Computational Linguistics, Empirical Methods in Natural Language Processing, Conference on Computational Linguistics, European Chapter of the Association for Computational Linguistics, Extending Database Technology, Transactions of the Association for Computational Linguistics, and Computational Linguistics (with more than 100 peer-reviewed publications).

ALFIO GLIOZZO is currently the principal researcher and technical program manager at IBM Research. Dr. Gliozzo has more than 20 years of research experience in generative AI, with a strong focus on natural language processing and knowledge graphs. He was a member of the Deep QA team that developed Watson, the IBM Question Answering system that defeated the Jeopardy! grand masters in 2011. Dr. Gliozzo leads significant research efforts aimed at providing natural language access to enterprise data lakes at IBM. He has authored more than 150 scientific publications and patents and has received several Outstanding Technical Achievement Awards from IBM for his contributions to the R&D of AI capabilities in IBM products. Additionally, he has taught cognitive computing at Columbia University for several years. Dr. Gliozzo is a member of ACM and regularly serves on the program committees of top AI conferences, such as AAAI and the International Joint Conferences on Artificial Intelligence. He received his PhD in communication technology from the University of Trento in 2005.

GREGORY F. LAWLER is the George Wells Beadle Distinguished Service Professor in Mathematics and in Statistics at the University of Chicago. He previously held professorships at Duke University and Cornell University. Dr. Lawler's expertise is probability and stochastic processes, with a particular interest in models that arise in statistical physics. He is the author of seven books (two co-authored) as well as numerous papers. Dr. Lawler is a member of NAS and AAA&S. His awards include the Wolf Prize in mathematics (2019) and the Polya Prize given by the Society for Industrial and Applied Mathematics (SIAM) (2006), and he was a plenary speaker at the International Congress of Mathematicians (2018). He is a fellow of both the Institute for Mathematical Statistics and the American Mathematical Society. He received a BA from the University of Virginia in 1976 and a PhD from Princeton University in 1979.

ANNA LYSYANSKAYA is the James A. and Julie N. Brown Professor of Computer Science at Brown University. A theme of her academic research is on balancing privacy with accountability, and specifically allowing users to prove that they are authorized even while not revealing any additional information about themselves. Dr. Lysyanskaya is a recipient of numerous awards from NSF, as well as industry grants from IBM, Google, and Facebook. She has served on the board of directors of IACR since 2012 and served as the program co-chair of the annual Crypto conference in 2023. In 2024, she was awarded the Levchin Prize for Real-World Cryptography. Dr. Lysyanskaya received an AB from Smith College in 1997, an SM from the Massachusetts of Technology (MIT) in 1999, and a PhD from MIT in 2002.

CHARIF MAHMOUDI is currently a senior security architect at Siemens Technology and an associate researcher at both the Telecommunications and Multimedia Laboratory at the University of Hassan II Casablanca and the Algorithmic Complexity and Logic Laboratory at Paris-Est Créteil University. Previously, he has held various positions in R&D, focusing on emerging networking technologies, mobile cloud computing, and software architecture. Dr. Mahmoudi is an expert in distributed systems,

Copyright National Academy of Sciences. All rights reserved.

cybersecurity, AI, and cloud computing, with a particular emphasis on securing cyber-physical systems and intelligent systems design. He has been recognized as a distinguished lecturer at both the University of North Texas and the Hassan II University of Casablanca and was a finalist for the Siemens Excellence Award. Additionally, he has served as an Associate of the Year at NIST. Dr. Mahmoudi obtained his PhD in formal verification of distributed systems from Paris-Est Créteil University, an MS in distributed systems from Paris 12 University, and a BS in computer science from École Supérieure d'Ingénierie en Sciences Appliquées. His doctoral research focused on the orchestration of mobile agents in communities. Notably, Dr. Mahmoudi has contributed to several research and industrial projects funded by organizations like the Defense Advanced Research Projects Agency (DARPA) and Siemens and has a robust record of publications in the field of distributed systems and cybersecurity. His professional service includes roles as a co-chair and technical program committee member for various IEEE conferences, and he has an extensive history of invited presentations and lectures at international conferences and universities.

LINDA R. PETZOLD is currently a distinguished professor in the Department of Mechanical Engineering and the Department of Computer Science and the director of the Computational Science and Engineering Graduate Emphasis at the University of California, Santa Barbara (UCSB). Dr. Petzold is a member of NAS and NAE, and a fellow of ACM, the American Society of Mechanical Engineers, SIAM, and the Association for the Advancement of Science (AAAS). She was named the UCSB Faculty Research Lecturer for 2011, was awarded the SIAM/ACM Prize for Computational Science and Engineering in 2013, received an honorary doctorate from Uppsala University in 2015, was awarded the SIAM Prize for Distinguished Service in 2016, and was awarded the IEEE Sydney Fernbach Prize in 2018. Her current research focuses on modeling, simulation, and data analytics of multiscale systems in biology and medicine.

MANAS N. RACHH is currently a research scientist in the Flatiron Institute's Center for Computational Mathematics. Before coming to the Flatiron, he was a Gibbs Assistant Professor in Applied Mathematics. Dr. Rachh's research interests include partial differential equations (PDEs) arising in mathematical physics, integral equation methods, robust computation of eigenvalues and eigenfunctions of elliptic PDEs, and the development of fast algorithms for applications in electrostatics, acoustics, viscous flow, electromagnetics, biomedical imaging, and data visualization. He obtained his BTech and MTech in aerospace engineering from the Indian Institute of Technology Bombay in 2011 and his PhD from the Courant Institute of Mathematical Sciences at NYU in 2015. Dr. Rachh is an organizer of a week-long workshop at Flatiron Institute titled "Computational Tools for PDEs with Complicated Geometries and Interfaces." The workshop is geared toward graduate students, postdoctoral researchers, and practitioners, and includes introductory talks on the basic mathematical foundation of integral equation methods, illustrations of their use in applications, and expert-run hands-on tutorials using a set of efficient software tools.

JEYAVIJAYAN (JV) RAJENDRAN is an associate professor and an ASCEND Fellow in the Department of Electrical and Computer Engineering at Texas A&M University. He obtained his PhD from NYU in August 2015. Dr. Rajendran's research interests include hardware security and computer security. His research has won the NSF CAREER Award in 2017, the Office of Naval Research Young Investigator Award in 2022, the IEEE CEDA Ernest Kuh Early Career Award in 2021, the ACM SIGDA Outstanding Young Faculty Award in 2019, the Intel Academic Leadership Award, the ACM SIGDA Outstanding PhD Dissertation Award in 2017, and the Alexander Hessel Award for the Best PhD Dissertation in the Electrical and Computer Engineering Department at NYU in 2016, and several best student paper awards. He organizes and has co-founded Hack@DAC, a student security competition co-located with the Design Automation Conference and Sushi.

Copyright National Academy of Sciences. All rights reserved.

DEBORAH SHANDS is currently a senior computer scientist at SRI International. Before joining SRI, Dr. Shands served as a program director for NSF's Secure and Trustworthy Cyberspace program. Prior to NSF, she worked as a senior security engineer for space systems at The Aerospace Corporation. She has expertise in systems security architecture and design, and scalable security administration of identity and access management. Dr. Shands's current work focuses on cybersecurity and privacy for digital credentials and identities. She is a member of ACM and is a recipient of a Distinguished Alumni Award from the Ohio State University College of Engineering and an IEEE Computer Society Outstanding Contribution Award for exemplary service. Dr. Shands received her BS in mathematics and computer science from the University of Minnesota and her PhD in computer and information science from Ohio State University in 1994.

EUGENE H. SPAFFORD is currently a professor at Purdue University, as well as the executive director emeritus of the Center for Education and Research in Information Assurance and Security. He has courtesy appointments in electrical and computer engineering, political science, philosophy, and communication. He has been on the faculty at Purdue for 37 years. Dr. Spafford has worked on issues in privacy, public policy, law enforcement, software engineering, education, social networks, operating systems, and cybersecurity. He has been involved in the development of fundamental technologies in intrusion detection, incident response, firewalls, integrity management, and forensic investigation. He is a fellow of AAA&S and AAAS; a Life Fellow of ACM, IEEE, and the (ISC)2; a Life Distinguished Fellow of the Information Systems Security Association; and a member of the Cyber Security Hall of Fame—the only person to ever hold all of these distinctions. In 2012, he was named one of Purdue's inaugural Morrill Professors—the university's highest award for the combination of scholarship, teaching, and service. In 2016, Dr. Spafford received the state of Indiana's highest civilian honor by being named as a Sagamore of the Wabash. He received his BS from the State University of New York at Brockport and his MS and PhD from Georgia Tech. Dr. Spafford then spent 18 months as a postdoctoral researcher in software engineering at Georgia Tech before joining the faculty at Purdue. He previously served on the National Academies' Panel on Review of the Information Technology Laboratory at the National Institute of Standards and Technology in 2018.

SHENGTAO WANG is currently the head of Quantum Algorithms and Applications at QuEra Computing Inc., which is a leader in commercializing quantum computers using neutral atoms. Dr. Wang is an expert in the development of near-term quantum algorithms and applications, in the areas of quantum optimization, quantum simulation, and quantum machine learning. He has more than 12 years of experience working in the field of quantum computing and quantum simulations. At QuEra, Dr. Wang leads a team of more than 10 senior scientists and engineers and has mentored more than 20 student interns as part of his team in the past 5 years. Prior to his position at QuEra, Dr. Wang was a postdoctoral scholar in the Department of Physics at Harvard University, where he made important contributions in developing near-term quantum optimization algorithms implementable on today's neutral-atom quantum computers. Dr. Wang received his BSc in 2011, with a double major in physics and mathematics, at Nanyang Technological University in Singapore and won the Top CN Yang Scholar Award. He received his PhD in physics at the University of Michigan, Ann Arbor, in 2017 and won the Wirt and Mary Cornwell Prize. Dr. Wang currently receives funding from DARPA, the National Energy Research Scientific Computing Center, and Wellcome Leap.

TOLGA YALCIN is currently a CPU Security Architect at Qualcomm Inc., San Diego. He has expertise in embedded and hardware security, applied cryptography, digital signal processing, and application-specific integrated circuit design. Dr. Yalcin received his PhD in microelectronics and microsystems from the Swiss Federal Institute of Technology Lausanne in 2007. Before joining Qualcomm in 2022, he worked for NXP, Northern Arizona University (as a research professor), and Google. He is a member of IEEE and has served as a program committee member and reviewer for major several conferences and journals in his area of expertise.

Copyright National Academy of Sciences. All rights reserved.

An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory: Fiscal Year 2024

SHERALI ZEADALLY is a university research professor and the University of Kentucky Alumni Association Endowed Professor at the University of Kentucky. He authored and co-authored more than 500 peer-reviewed publications, of which 371 papers have appeared in peer-reviewed international journals and magazines. This also includes 40 peer-reviewed book chapters. Dr. Zeadally has authored and co-edited 8 books. He has received 13 best paper awards with 11 of them from well-known peer-reviewed international journals. He was named a highly cited researcher in computer science in 2020, 2021, 2022, and 2023 by Clarivate. He received more than 60 awards, honors, and prestigious fellowships nationally and internationally for his outstanding research, teaching, and service in his career. Dr. Zeadally has received several outstanding research awards from the University of Kentucky, nationally, and internationally. At the University of Kentucky, he won several university-wide awards, including the University Research Professor Award, the Albert D. and Elizabeth H. Kirwan Memorial Prize, the Alumni Professorship Award, the Global Impact Award for Distinguished Faculty Achievements in International Research and Scholarship, the Excellent Undergraduate Research Mentor Award, and the Ken Freedman Outstanding Faculty Advisor Award. At the national level, he won the prestigious IEEE Region 3 Outstanding Engineer Award and the IEEE–USA George F. McClure Citation of Honor. At the international level, he received the prestigious Communications Software Technical Achievement Award from the IEEE Communications Society Communications Software Technical Committee in 2015 and the IEEE Smart Computing Special Technical Community Life-Career Award in 2023. He has also received several research mentor and advising awards (all of them nominated by undergraduate and graduate students) from the University of Kentucky for his outstanding mentoring and advising efforts. He has received multiple outstanding teaching awards (two excellence in teaching awards, a President's award for excellence in teaching, and a Great Teacher Award) at both undergraduate and graduate levels. Dr. Zeadally has made numerous service contributions as the editor-in-chief of an international peer-reviewed journal; an associate editor and editorial board member of more than 15 peer-reviewed academic journals; a chair, co-chair, and technical program committee member of several peer-reviewed conferences; and a grant reviewer for more than 40 grant funding agencies nationally and internationally. Dr. Zeadally earned his bachelor's degree in computer science from the University of Cambridge, England. He also received a doctoral degree in computer science from the University of Buckingham, England, followed by postdoctoral research at the University of Southern California. His research interests include cybersecurity, privacy, Internet of Things, and computer networks (vehicular networks and sensor networks).

MARY ELLEN ("MEZ") ZURKO is a technical staff member at the MIT Lincoln Laboratory. Ms. Zurko has worked in product development, early product prototyping, and research and has more than 20 patents. She defined the field of user-centered security in 1996 and has worked in cybersecurity for more than 35 years. Ms. Zurko was the security architect of one of IBM's earliest clouds. She was a founding member of the National Academies' Forum on Cyber Resilience and serves as a Distinguished Expert for the National Security Agency's Best Scientific Cybersecurity Research Paper competition. Her research interests include unusable security for attackers, Zero Trust architectures for government systems, security development and code security, authorization policies, high-assurance virtual machine monitors, the web, and public key infrastructure. Ms. Zurko received an SB and an SM in computer science from MIT.

Copyright National Academy of Sciences. All rights reserved.