2022 Cybersecurity & Privacy Annual Report

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST SPECIAL PUBLICATION 800-225

NIST Special Publication
NIST SP 800-225

Fiscal Year 2022 Cybersecurity and Privacy Annual Report

Patrick O’Reilly, Editor
Computer Security Division
Information Technology Laboratory

Kristina Rigopoulos, Editor
Applied Cybersecurity Division
Information Technology Laboratory

Co-Editors:
Larry Feldman
Greg Witte
Huntington Ingalls Industries

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-225

May 2023

U.S. DEPARTMENT OF COMMERCE
Gina M. Raimondo, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

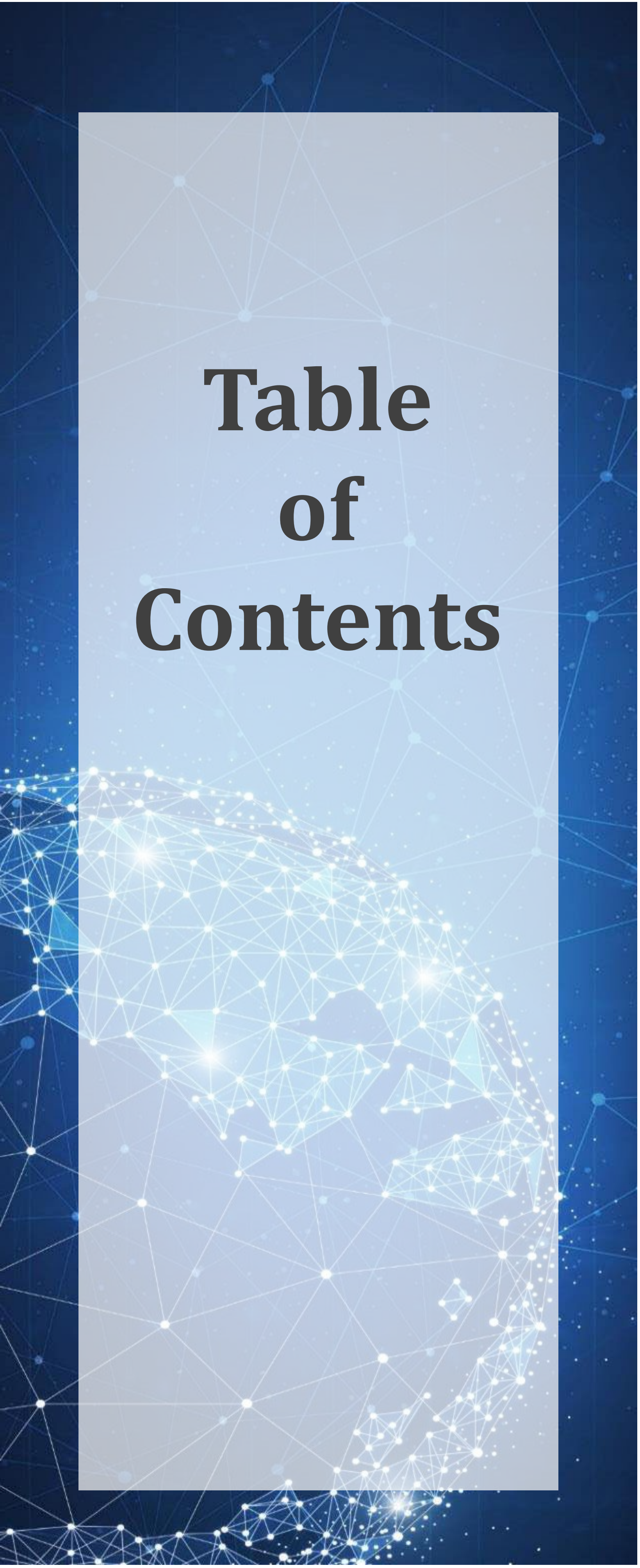


Table of Contents

Priority Areas

Foreword

FOREWORD

Nelson Mandela famously said, “Remember to celebrate milestones as you prepare for the road ahead.”
This year, we celebrated a major milestone that we’re proud of: 50 years of cybersecurity at NIST. Over the last five decades, we have conducted research and developed guidance that has led to extraordinary advancements in cybersecurity.

Many of these advancements have taken on new life over the years as the world of cybersecurity shifts and adjusts. We look forward to outlining our accomplishments each year in these Annual Reports as we share how our dynamic projects help advance technology, cybersecurity and privacy standards and guidelines, and measurement science for all.

You’ll notice that this year’s Annual Report has a new look and feel. We are debuting a simpler format with less text and more pointers to our helpful and robust websites, and we organized the publication into seven key categories (*see our table of contents for a list, and read about each one throughout this report*).

This past year, NIST conducted research and demonstrated practical applications in several key priority areas, including Post Quantum Cryptography (and the selection of PQC algorithms for standardization); an update to the NIST Cybersecurity Framework (CSF 2.0), including new CSF profiles; software and supply chain cybersecurity; our Internet of Things (IoT) cybersecurity guidelines work; launching a new comment site for our security and privacy controls and baselines (so we can get our resources into the hands of practitioners faster and improve the user experience for our customers); and much more.

We are always learning, growing, and creating, so sometimes we forget to take a minute to reflect. This year, we enjoyed doing just that as we celebrated the very milestones that make us unique.

- **Kevin Stine**, **NIST Chief Cybersecurity Advisor**

How did we celebrate our 50th anniversary of cybersecurity this year?

- We launched a new NIST Cybersecurity Program History and Timeline tool, which provides an overview of NIST’s major cybersecurity research projects, programs, and – ultimately – history.
- We set up a dedicated anniversary website that has everything in one place – blog posts, event details, and resources.
- We shared and collaborated on our cybersecurity Twitter account using the hashtag #NISTcyber50th all year.

Cryptography

CRYPTOGRAPHY

Cryptography is foundational to our security and data protection needs. The standards, guidelines, recommendations, and tools provided by NIST's Cryptography priority area enable trustworthy assurance of integrity and confidentiality in all types of information and technology – now and in the future.

Major Accomplishments in FY 2022:

- The Post-Quantum Cryptography team announced the third-round selection and the fourth-round candidates. The call for additional signatures was released. Standards development on the selected algorithms is underway.
- The Lightweight Cryptography Project continued to evaluate the finalist algorithms to prepare for the final selection. The fifth Lightweight Cryptography Workshop was held.
- NIST's Crypto Publication Review Board completed two reviews, and seven reviews are in progress to update and modernize the portfolio of cryptographic standards.
- NIST continued to explore multi-party threshold cryptography through workshops, calls for feedback on criteria for threshold schemes, and other industry collaboration.

Learn more about this priority area

Image credit: Shutterstock

> **NIST is proud to have achieved the milestone of selecting the algorithms which will help protect our sensitive data against the possibility of future attacks from quantum computers.**
>
> ***- Dustin Moody, NIST PQC Project Lead***

Education, Training & Workforce

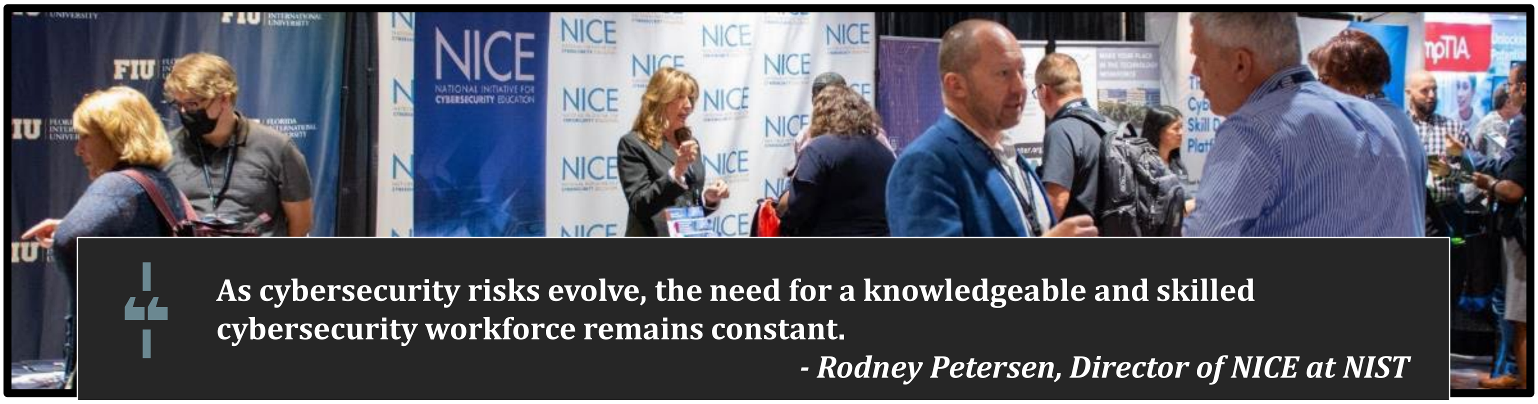
EDUCATION, TRAINING & WORKFORCE

Energizing, promoting, and coordinating the workforce are key priorities for NIST. The National Initiative for Cybersecurity Education (NICE) supports a robust community that works together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

Major Accomplishments in FY 2022:

- NICE released the National K12 Cybersecurity Education Roadmap with five major elements and accompanying strategies.
- The NICE Community Coordinating Council launched five project teams that each support objectives from the NICE Strategic Plan.
- NICE launched the Cybersecurity Apprenticeship Finder and supported a 120-Day Cybersecurity Apprenticeship Sprint in partnership with the U.S. Department of Labor.
- A report, "Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework", was submitted to Congress.
- In response to the FY 2021 National Defense Authorization Act, NICE submitted a report to Congress on cybersecurity proficiencies and published cybersecurity career pathways information.
- The Small Business Cybersecurity Corner released a series of videos with companion discussion guides on ransomware, phishing, and multi-factor authentication.
- NIST continued to bring together the community through events, including the Federal Cybersecurity Workforce Summit and Webinars, Federal Information Security Educators (FISSEA) Forums, NICE Webinar Series, Cybersecurity Career Awareness Week, and by supporting the NICE Conference, NICE K12 Conference, and US Cyber Games through cooperative agreements.

Learn more about these priority areas



> **As cybersecurity risks evolve, the need for a knowledgeable and skilled cybersecurity workforce remains constant.**
> ***- Rodney Petersen, Director of NICE at NIST***

Image credit: Florida International University

Identity & Access Management

IDENTITY & ACCESS MANAGEMENT

Identity and Access Management (IAM) is the cornerstone of data protection, privacy, and security. NIST's IAM priority area provides the research, guidance, and technology transition activities to help ensure that the right humans, devices, data, and processes have the right access to the right resources at the right time.

Major Accomplishments in FY 2022:

- A third revision of the Personal Identity Verification of Federal Employees standard was published, which specifies secure and reliable forms of identity credentials for federal employees and contractors who need access to federal facilities and applications.
- The draft of NIST's Digital Identity Guidelines was completed, incorporating comments submitted in response to the June 2020 Request for Comments (RFC), lessons learned from federal agencies and industry, and new content about emerging technologies, threats, and policies.
- Part 8 of the Face Recognition Vendor Test (FRVT) was published. This report compiles and analyzes demographic summary measures for how face recognition false positive and false negative error rates differ across age, sex, and race-based demographic groups. This is a key step toward a metric that can be used to summarize demographic differentials, support standards development for measuring performance, and drive improvements in the technology.
- Guidance was provided for the implementation of DevSecOps primitives for reference platforms that host cloud-native applications with the publication of Application of DevSecOps Using a Service Mesh in Microservices-Based Infrastructure.
- NIST contributed to and helped finalize the international standard for Mobile Driving License (mDL) Applications, developed a reference implementation to test the standard, and created security and privacy considerations for the mDL ecosystem.

Learn more about this priority area

Image credit: Shutterstock

> **NIST's Identity & Access Management Program is a cornerstone for government services. From Zero Trust to benefits distribution, some of the most critical aspects of government rely on our research and guidance….**
>
> ***- Ryan Galluzzo, NIST Digital Identity Program Lead***

Privacy

PRIVACY

Privacy is integral to the trust that supports the growth of the digital economy and improves our quality of life. NIST has prioritized Privacy Engineering to support measurement science and system engineering principles through frameworks, risk models, and guidance that protect privacy and civil liberties.

Major Accomplishments in FY 2022:

- Numerous Privacy Framework resources were released, including Spanish and Portuguese translations of the Privacy Framework Quick Start Guide and a webinar on using regulatory crosswalks for Framework implementation.
- NIST's differential privacy blog series was completed, and in-depth differential privacy guidelines are in development (a draft for public comment is anticipated in FY 2023).
- The NIST Privacy Workforce Public Working Group (PWWG) was launched, which now has 800+ members from across the globe. Project teams are currently working on defining tasks, knowledge, and skills aligned with the Privacy Framework and the NICE Framework to support the growth of a workforce capable of managing privacy risks. Two of an anticipated ten PWWG project teams have completed their work, and three additional have launched.
- Co-sponsored by NIST, the U.S. partnered with the U.K.'s Center for Data Ethics and Innovation to launch a Privacy-Enhancing Technologies Prize Challenge to advance privacy-preserving federated learning.
- The Privacy Engineering Program continues to collaborate across NIST programs and priority areas. NIST also leads external efforts to advance privacy, including co-chairing Privacy Research & Development and Privacy-Preserving Data Sharing and Analytics Interagency Working Groups.

Learn more about this priority area

Image credit: Shutterstock

> **"The NIST Privacy Framework, published in January 2020, is quickly becoming the mainstream control set for organizations to align with when assessing their data privacy posture, developing readiness roadmaps, and maturing their privacy program."**
>
> ***-JD Supra, LLC***

Risk Management & Measurement

RISK MANAGEMENT AND MEASUREMENT

Organizations must balance a rapidly evolving cybersecurity and privacy threat landscape with the need to fulfill enterprise mission and business requirements. This evolution increasingly calls for a collaborative approach to managing discipline-specific enterprise risks. Risk management is integrated into NIST standards and guidelines to help better understand, measure, manage, and reduce cybersecurity and privacy risk in a larger context.

Major Accomplishments in FY 2022:

- NIST kicked off the Journey to CSF 2.0 with a Request for Information (RFI), a summary analysis document of the RFI responses, and a workshop with 3,900+ attendees from 100 countries. More planning is now underway for additional workshops and drafts.
- Updated guidance on assessing security and privacy controls was released, featuring updated assessment procedures to better enable automation.
- Guidance on managing cybersecurity risk in supply chains for all levels of an organization was released with specific sections focused on securing software supply chains. Additionally, NIST collaborated with software developers, service providers, and users to develop secure software development guidance that is now mandatory for federal agency software acquisition and use.
- New guidance and example implementations were developed and released to demonstrate how organizations can verify that the internal components of their computing devices are genuine and have not been tampered with.

Learn more about this priority area

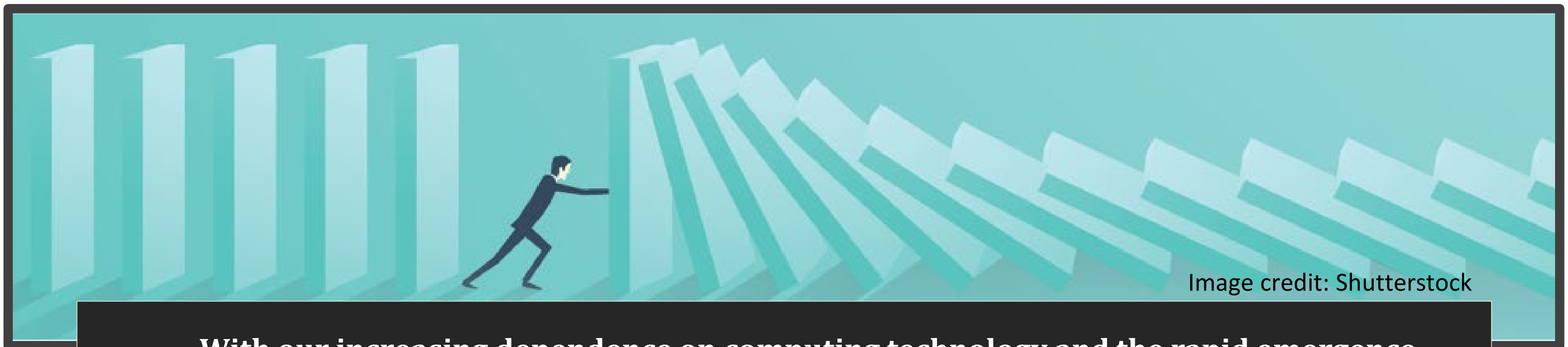


Image credit: Shutterstock

> **With our increasing dependence on computing technology and the rapid emergence of cyber-physical systems – from medical devices to automobiles to the electric grid – managing cybersecurity and privacy risk is an essential component in the safe and effective use of those systems. We are committed to our stakeholder-driven, collaborative, and thorough approach.**
>
> ***- Ron Ross, NIST Fellow***

Trustworthy Networks & Platforms

TRUSTWORTHY NETWORKS AND PLATFORMS

Each of us relies on the hardware, software, and networks that form the fabric of our digital ecosystems. NIST's Trustworthy Networks and Trustworthy Platforms priority areas support research and practical implementation guidance to ensure secure, reliable, and resilient technology across industry sectors.

Major Accomplishments in FY 2022:

- NIST published guidance to enhance and strengthen the security and integrity of the software supply chain in support of Executive Order (EO)14028. This effort included cybersecurity supply chain risk management practices and guidelines for software developer verification, systems security engineering, and secure software development.
- Hardware security mechanisms and governance safeguards guidance was finalized to measure and attest to the integrity of the platform in an infrastructure-as-a-service (IaaS) cloud deployment model and other multi-tenant cloud environments.
- The development of the Cybersecurity for IoT program has progressed through stakeholder engagement, guidance for consumers of IoT products and federal agencies, and practical guidance for securing industrial internet of things (IIoT) devices (e.g., distributed energy resources).

Learn more about the Trustworthy Networks and Platforms priority areas

> **Leverage measurement science, guidelines, and standards to foster the adoption of innovative and trustworthy information and communication technology.**
>
> ***- Murugiah Souppaya, NIST Computer Scientist***

Image credit: Shutterstock

Usable Cybersecurity

USABLE CYBERSECURITY

The mission of the Usable Cybersecurity priority area is to "champion the human in cybersecurity." Through human-centered research and projects, the usability team seeks to better understand and improve users' cybersecurity interactions and empower people to be active, informed participants in cybersecurity.

Major Accomplishments in FY 2022:

- NIST received a provisional patent for the Phish Scale – a method to help organizations contextualize phishing training click rates. The scale was further expanded based on real-world data and feedback from the growing number of organizations that have adopted the Phish Scale.
- A parent-child study examining youths' cybersecurity and privacy perceptions, knowledge, and behaviors found that conversations with parents were key to youth gaining solid understandings regarding the topics. Results were shared in research and government forums.
- A research study identified the approaches and challenges of U.S. Government cybersecurity awareness programs – including emphasis on compliance rather than impact – and informed new government awareness and training guidelines.
- Survey findings on consumer perceptions and experiences with updates for smart home devices revealed a lack of transparency and user misconceptions. Results informed Internet of Things cybersecurity guidelines and labeling efforts.

Learn more about this priority area

> **We amplify the voices and needs of people within a field that is most often viewed through a technology-dominant lens.**
>
> ***- Julie Haney, NIST Usable Cybersecurity Program Lead***

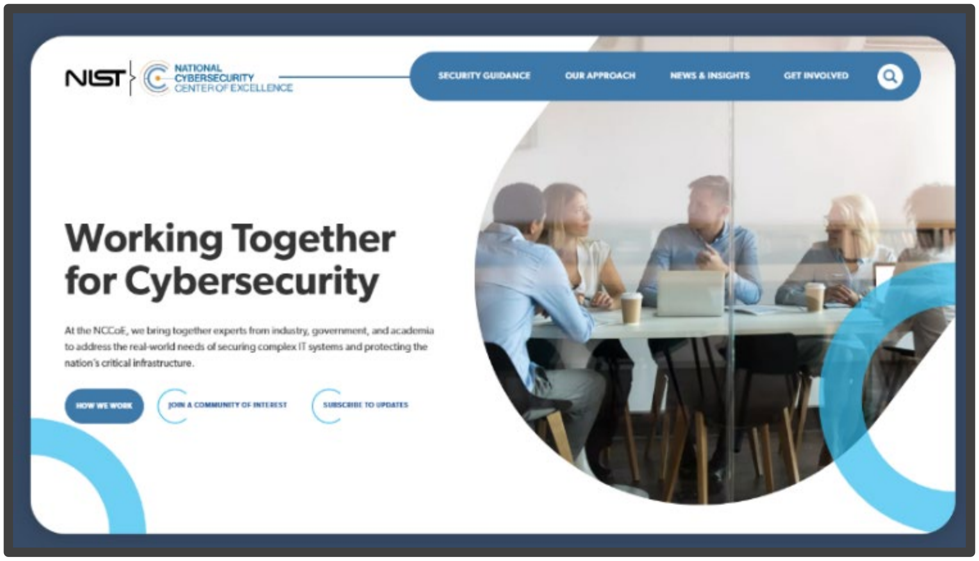
Image credit: Shutterstock

National Cybersecurity Center of Excellence (NCCoE) Summary

SUMMARY OF THE NCCOE

> **The NCCoE brings together members of industry, government, and academia to address the real-world needs of securing complex systems and protecting the Nation's critical infrastructure.**

- **Happy Birthday, National Cybersecurity Center of Excellence (NCCoE)!** NCCoE celebrated its 10-year anniversary in FY 2022. The NCCoE was established in 2012 through a partnership among NIST, the State of Maryland, and Montgomery County, MD.
- **Practical, standards-based guidance.** The NCCoE published 33 publications in FY 2022 on topics ranging from enterprise patch management, trusted cloud, securing telehealth, zero trust, mobile device security, supply chain integrity, and much more. View our full list of publications here.
- **Exploring new areas.** We launched new projects in the areas of hybrid satellite networks, identity, telehealth smart home integration, post-quantum cryptography, cybersecurity of genomic data, artificial intelligence, and software supply chain, to name a few.
- **New look, same great information.** We launched a redesigned NCCoE website to improve the user experience.
- **Take a virtual look inside the NCCoE labs.** We developed a virtual lab tour series. Explore the work being done in each lab, meet our subject-matter experts, and learn what sector or technology challenges our projects are addressing here.



Working Together for Cybersecurity

At the NCCoE, we bring together experts from industry, government, and academia to address the real-world needs of securing complex IT systems and protecting the nation's critical infrastructure.

OPPORTUNITIES TO ENGAGE WITH NIST ON CYBERSECURITY & PRIVACY

Collaborators and researchers are the driving force behind NIST's programs. NIST depends on developers, providers, and everyday users of cybersecurity and privacy technologies and information to guide our priorities.

- Details on engaging with NIST on cybersecurity and privacy are available here.
- Many NIST projects are supported by guest researchers, both foreign and domestic.
- The Pathways Program supports federal internships for students and recent graduates.
- NIST funds industrial and academic research in several ways:
  - The Small Business Innovation Research Program (SBIR) funds research and development proposals.
  - NIST offers grants to encourage work in the fields of precision measurement, fire research, and materials science. For general information on NIST's grant programs, please contact Mr. Christopher Hunton via grants@nist.gov.
- The Information Technology Laboratory (ITL) Speakers Bureau enables engagement with universities and colleges to raise student and faculty awareness about the exciting work going on at NIST and motivate them to consider pursuing opportunities to work with ITL.
- More information about our research, projects, publications, and events can be found on the NIST Computer Security Resource Center (CSRC) website.

Image credit: Canva

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

How to Cite this NIST Technical Series Publication

O'Reilly PD, II, Rigopoulos KG, Feldman L, Witte GA (2023) Fiscal Year 2022 Cybersecurity and Privacy Annual Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-225. https://doi.org/10.6028/NIST.SP.800-225.

Disclaimer

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Acknowledgments

The editors would like to thank their NIST colleagues by extending special recognition and appreciation for Victoria Yan Pillitteri, Isabel Van Wyk, Jeffrey Marron, Matthew Scholl, Kevin Stine, Sara Kerman, Sheryl Taylor, and Jim Foti for reviewing and providing valuable feedback, writing input, and administrative support for this Annual Report.

Trademark Information

All names are trademarks or registered trademarks of their respective owners.

Abstract

During Fiscal Year 2022 (FY 2022) – from October 1, 2021, through September 30, 2022 – the NIST Information Technology Laboratory (ITL) Cybersecurity and Privacy Program successfully responded to numerous challenges and opportunities in security and privacy. This Annual Report highlights the FY 2022 research activities for the ITL Cybersecurity and Privacy Program, including: the ongoing participation and development of international standards; research and practical applications in several key priority areas (e.g., Post Quantum Cryptography, updating the NIST Cybersecurity Framework (CSF 2.0) and some new CSF profiles); accomplishments in the area of improving software and supply chain cybersecurity; IoT cybersecurity guidelines work; National Cybersecurity Center of Excellence (NCCoE) projects, and setting up a new comment site for NIST's Risk Management Framework work. NIST also celebrated a 50th anniversary in cybersecurity and the NCCoE celebrated a 10-year anniversary since inception.

Keywords

annual report; cybersecurity; cybersecurity program; Federal Information Security Management Act; FISMA; privacy; program highlights; information security; Information Technology Laboratory; ITL; program accomplishments.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

NIST
INFORMATION
TECHNOLOGY
LABORATORY