2023 Cybersecurity & Privacy Annual Report

NIST SPECIAL PUBLICATION 800-229

NIST Special Publication 800
NIST SP 800-229

Fiscal Year 2023 Cybersecurity and Privacy Annual Report

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

Kristina Rigopoulos, Editor
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-229

May 2024

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

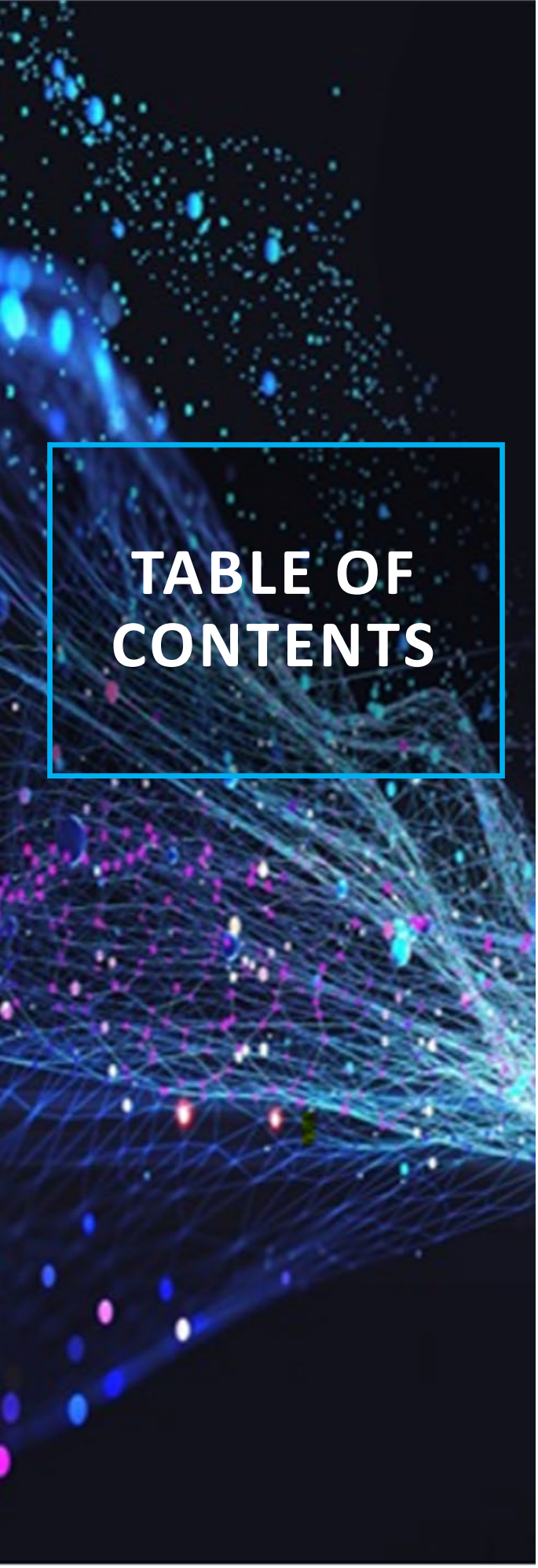
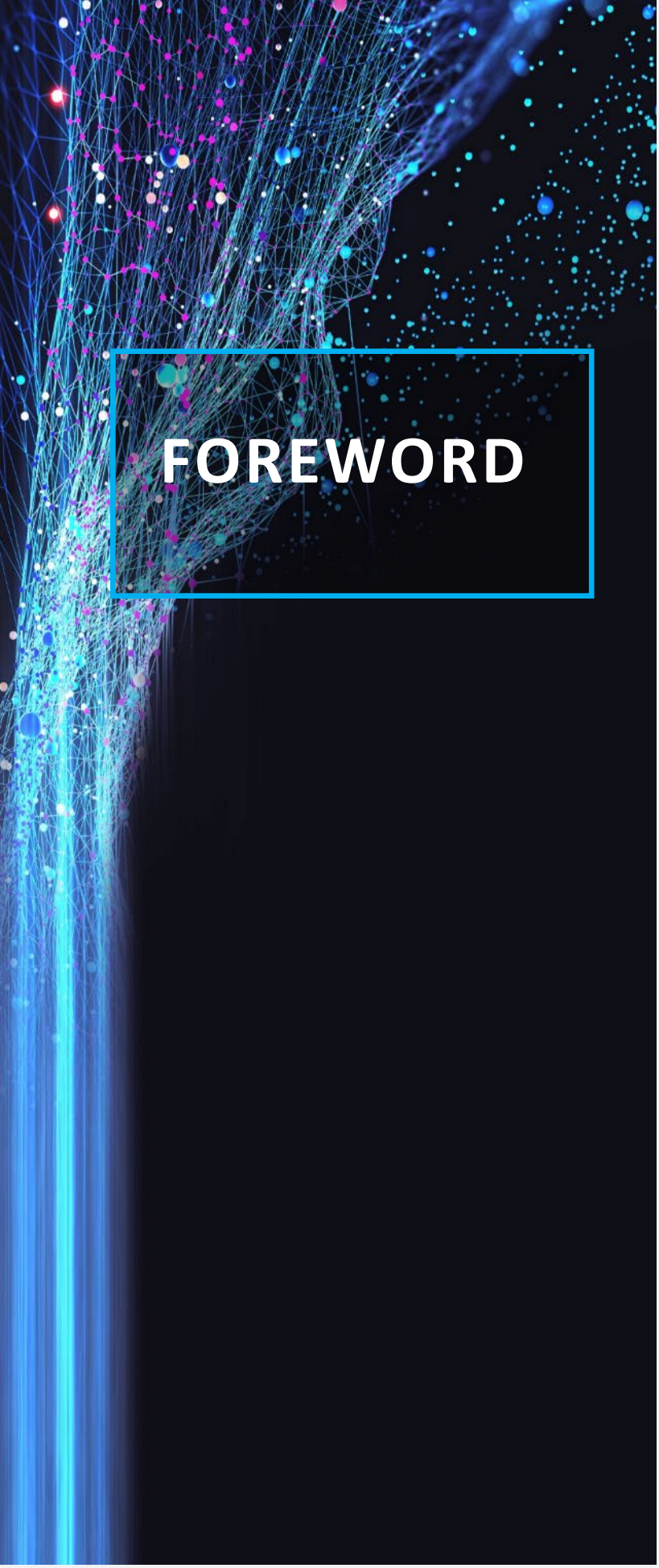


TABLE OF CONTENTS



FOREWORD

This year has been one to remember!

As we wrapped up our celebration of 50 years of work in cybersecurity, we continued to prioritize our quest for deep collaboration with the community and seamless coordination across NIST throughout 2023.

Our research and demonstrated practical applications work spanned across several key priority areas, which are outlined in this report—with hyperlinked pointers to more specifics if you'd like to dig deeper or learn more.

NIST's work meshes well with – and is a key part of – the National Cybersecurity Strategy and the related Implementation Plan. NIST is singled out for its work related to international standards, an area that we have prioritized and is yielding notable results.

In the same vein, the U.S. Government National Standards Strategy for Critical and Emerging Technology released in 2023, cites Cybersecurity and Privacy as "cross-cutting issues that are critical to enabling the development and deployment of emerging technologies and promote the free flow of data and ideas with trust." NIST has been assigned to lead the federal government in advancing that strategy.

We hope that you will take the time to review some of the key highlights of our cybersecurity and privacy accomplishments from FY 2023 and to explore some of the projects that we are so proud of.

Most importantly, we look forward to learning more from you as our journeys together continue. As ever, we appreciate your support and hope that you are making the best possible use of NIST's work.

~ Kevin Stine
NIST Chief
Cybersecurity Advisor

Cryptography

Credit: ShutterStock

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 2023:

- The Post-Quantum Cryptography (PQC) team hosted the Fourth PQC Standardization Conference in November 2022. In response to the Call for Additional Signatures, 40 candidate algorithms were submitted, and the first three draft PQC standards were released for public comment.
- The Lightweight Cryptography team announced the decision to standardize the Ascon family for lightweight cryptography applications and published IR 8454, *Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*, which describes the selection process. The team also hosted the Sixth Lightweight Cryptography Workshop.
- The Multi-Party Threshold Cryptography (MPTC) and Privacy-Enhancing Cryptography (PEC) projects jointly released the initial public draft of IR 8214C, *NIST First Call for Multi-Party Threshold Schemes* (MPTS). The document's scope includes advanced techniques, such as fully homomorphic encryption, zero-knowledge proofs, and the building blocks of secure multi-party computation. As part of an effort to obtain public comments, NIST hosted the MPTS 2023 workshop and three events of the Special Topics on Privacy and Public Auditability (STPPA).
- NIST's Crypto Publication Review Board completed seven publication reviews, and five reviews are in progress to update and modernize the portfolio of cryptographic standards.

Learn more about this priority area

Education, Training & Workforce Development

Credit: iKeepSafe

EDUCATION, TRAINING & WORKFORCE

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

Major Accomplishments in FY 2023:

- On December 5, 2022, the NICE Workforce Framework for Cybersecurity (NICE Framework) K12 FAQ was released at the NICE K12 Cybersecurity Education Conference in St. Louis, MO.
- The NICE Framework continued to be updated throughout FY 2023, including calls for comments on updated materials. IR 8355, *NICE Framework Competencies Areas: Preparing a Job-Ready Cybersecurity Workforce*, was published on June 1, 2023.
- Diversity, equity, inclusion, and accessibility (DEIA) in the cybersecurity workforce and education were key efforts in 2023. NICE released a DEIA resource page and launched a new Diversity and Inclusion Community of Interest.
- The Small Business Cybersecurity Corner launched a new Community of Interest with the National Cybersecurity Center of Excellence (NCCoE) and participated in various events throughout the year to showcase and share resources.
- NIST has continued to bring the community together throughout the year with the Federal Information Security Educators (FISSEA) Forums, NICE Webinars Series, and Cybersecurity Career Week and by supporting other events through cooperative agreements, such as the NICE Conference, NICE K12 Conference, and the US Cyber Games.

Learn more about this priority area

Emerging Technologies

Credit: ShutterStock

EMERGING TECHNOLOGIES

The rapid evolution of technology brings both extraordinary opportunities and unavoidable challenges. At NIST, our cybersecurity researchers study these emerging technologies to understand their security and privacy capabilities, vulnerabilities, configurations, and overall structures in order to develop standards, guidelines, and references for improving their approaches to cybersecurity before they are deployed.

Major Accomplishments in FY 2023:

Cybersecurity projects in Strategic and Emerging Research Initiatives (SERI) for Autonomous Vehicles (AV) included the following:

- A workshop on Standards and Performance Metrics for On-Road Automated Vehicles was held to solicit stakeholder feedback on the challenges and opportunities in developing standards and performance metrics for this complex interdisciplinary field.
- The NIST AV Community of Interest (COI) has over 300 participants and continues to serve as a communications channel for NIST activities in the automotive industry.
- The Capabilities of Dioptra — an experimental testbed for machine learning algorithms — continued to expand.
- NIST built a SERI prototype that measures the sensitivity of uncertainty estimation in computer vision models for autonomous driving.
- Project researchers collaborated with external partners with appropriate datasets and computational resources.

In March 2023, the Adversarial Artificial Intelligence (AI) team released the initial public draft of AI 100-2 E2023, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, for public comment. Leading experts in the industry were invited to assist with adjudicating the public feedback to prepare a final AI 100-2 document, which is slated to be published in early 2024.

Learn more about this priority area

Human-Centered Cybersecurity

Credit: ShutterStock

HUMAN-CENTERED CYBERSECURITY

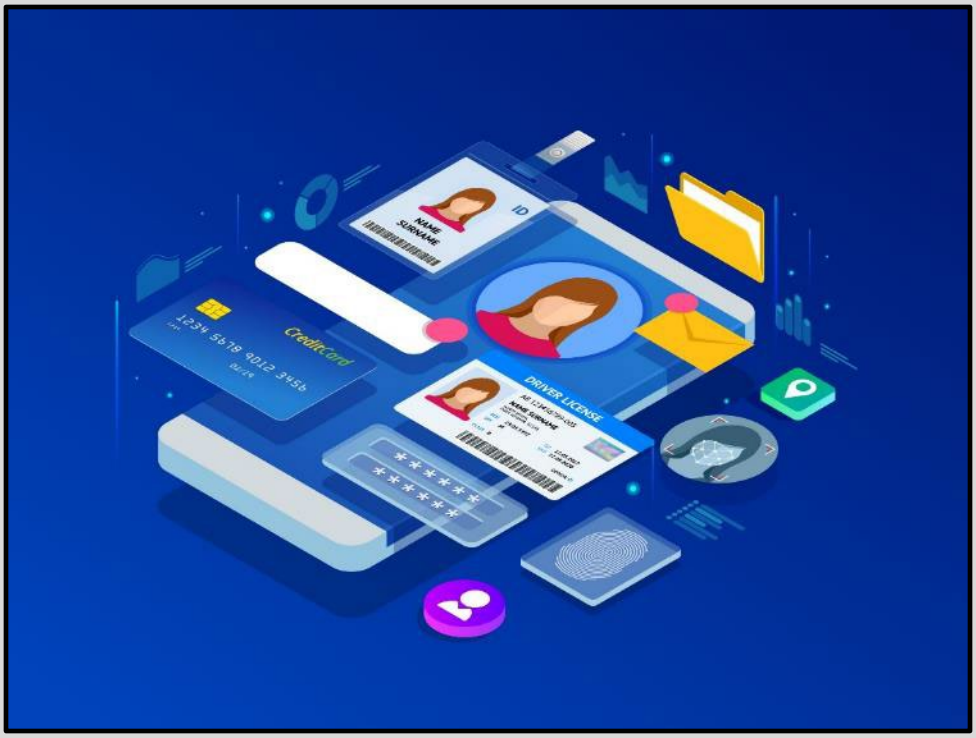
The mission of the Human-Centered Cybersecurity priority area is to "champion the human in cybersecurity." Through research and other human-centered projects, the program team seeks to better understand and improve people's cybersecurity interactions, empowering them to be active, informed participants in cybersecurity.

Major Accomplishments in FY 2023:

- An interview study of parent-child pairs shed light on how parents can best support their children's online privacy, security, and safety. The research insights are informing NIST's participation and contribution to the interagency Task Force on Kids Online Health and Safety.
- The phishing project team was awarded a U.S. Department of Commerce Gold Medal for creating the Phish Scale — a revolutionary tool to rate socially engineered email attacks to strengthen an organization's security posture. The scale has been adopted by security training coordinators in public- and private-sector organizations, both domestically and internationally.
- A role-based training study provided insights into the approaches and challenges faced by federal organizations when implementing cybersecurity training activities. The research resulted in the development of recommendations and resources to assist organizations in improving their role-based training activities.
- A widely distributed article and handout titled, "Users Are Not Stupid: Six Cybersecurity Pitfalls Overturned," provided cybersecurity practitioners with evidence-based recommendations on how they can consider the human element in their work.

Learn more about this priority area

Identity and Access Management



Credit: ShutterStock

IDENTITY AND ACCESS MANAGEMENT

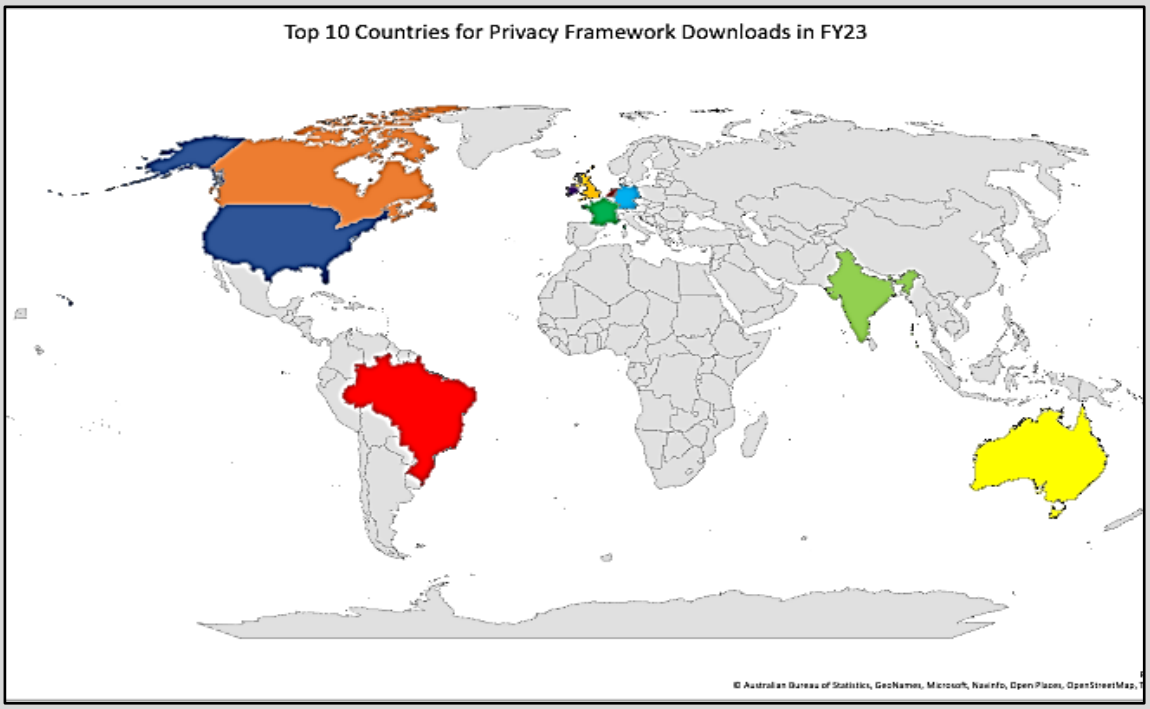
Identity and access management (IAM) is the cornerstone of data protection, privacy, and security. NIST's IAM priority area provides the research, guidance, and technology transition activities to help ensure that the right humans, devices, data, and processes have the right access to the right resources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

Major Accomplishments in FY 2023:

- NIST published draft revisions of all four volumes of SP 800-63-4, *Digital Identity Guidelines*, to advance modern digital identity controls.
- NIST's Identity and Access Management (IAM) team published draft SP 800-157-1, *Guidelines for Derived Personal Identification Verification (PIV) Credentials*, which features expanded authenticators, and draft SP 800-217, *Guidelines for PIV Federation*, which advances interoperable identity in the federal enterprise.
- Two Face Analysis Technology Evaluation (FATE) reports were published: NIST IR 8485, *Part 11: Face Image Quality Vector Assessment: Specific Image Defect Detection*, focused on face image quality and the detection of specific image defects that negatively impact matching accuracy, and NIST IR 8491, *Part 10: Performance of Passive, Software-based Presentation Attack Detection (PAD) Algorithms*, focused on PAD, which detects fake face images.
- NIST developed a secure federated data-sharing system (SFDS), which is now in advanced prototype form.
- NIST's IAM team published SP 800-207A, *A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments*.
- A draft IAM Roadmap that highlights programmatic and strategic priorities was released to help prioritize and strategically align identity projects.
- NIST's IAM team contributed to the development of the Mobile Drivers' License Application standard (ISO/IEC 18013-7) and developed a reference implementation for the standard to facilitate testing and the certification of products.

Learn more about this priority area

Privacy



48,221 Privacy Framework Downloads in FY23.

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 2023:

- The NIST Privacy Workforce Public Working Group has nearly completed the first draft of the Privacy Workforce Taxonomy and created more than 700 task, knowledge, and skill statements thus far.
- Co-sponsored by NIST, the U.S. partnered with the U.K.'s Center for Data Ethics and Innovation and completed the Privacy-Enhancing Technologies Prize Challenge to advance privacy-preserving federated learning.
- NIST's Privacy Engineering Program (PEP) continues to collaborate with other NIST programs, including the NCCoE, the Cryptography Technology Group, and the Risk Management Framework program. NIST leadership with external organizations is ongoing, including co-chairing the Networking and Information Technology Research & Development (NITRD) Privacy Research & Development Interagency Working Group and Coalition for Health AI Privacy and Security Working Group.

Learn more about this priority area

Risk Management

Credit: ShutterStock

RISK MANAGEMENT

Organizations must balance an evolving cybersecurity and privacy threat landscape with the need to fulfill mission and business requirements — an effort that increasingly calls for a collaborative approach to managing risks. Risk management is integrated into NIST standards and guidelines to help organizations understand, measure, manage, and reduce cybersecurity and privacy risks in a larger context.

Major Accomplishments in FY 2023:

- NIST continued the Journey to Cybersecurity Framework (CSF) 2.0 by releasing a CSF 2.0 Concept Paper, publishing a discussion draft of the CSF 2.0 Core, and issuing a draft CSF 2.0 with Core Implementation examples. Additionally, NIST published an analysis of comments received on each draft and hosted two hybrid workshops (1st workshop & 2nd workshop).
- NIST continued to lead and support community engagement on cybersecurity supply chain risk management through the Software and Supply Chain Assurance (SSCA) Forum, support the Federal Acquisition Security Council, and refine supply-chain guidance in SP 800-161 Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.
- NIST issued a working draft of the SP 800-55 Rev. 2, *Performance Measurement Guide for Information Security* for community discussion and feedback and hosted a cybersecurity measurement workshop on the current state of cybersecurity performance measurement, needs, and path forward.
- NIST initiated updates to the Protecting Controlled Unclassified Information (CUI) Series, issued a pre-call for comment, released an initial public draft of SP 800-171r3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and hosted a webinar to provide an overview of the draft.
- NIST launched the Cybersecurity & Privacy Reference Tool (CPRT) — an online application that provides NIST guidance and frameworks in a consistent format for reference data and allows users to understand the relationships between NIST resources.
- NIST continued the development of the Open Security Controls Assessment Language (OSCAL) — a set of eXtensible Markup Language (XML), JavaScript Object Notation (JSON), and Ain't Mark-up Language (YAML) formats that provide machine-readable representations of security and privacy information relative to the implementation, assessment, and continuous monitoring of systems. NIST SP 800-53, SP 800-53A, and SP 800-53B are available in OSCAL format, and programs such as FedRAMP are leveraging OSCAL.

Learn more about this priority area

Trustworthy Networks and Platforms

Credit: ShutterStock

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 2023:

- NIST published a practice guide for SP 1800-34, *Validating the Integrity of Computing Devices*, to mitigate cyber supply chain risks, such as counterfeiting, tampering, and the insertion of unexpected firmware. The practice guide demonstrates how organizations can verify that the internal components of the computing devices they acquire (e.g., laptops, servers) are genuine and have not been tampered with.
- Trust in endpoint devices can be achieved by following SP 800-124r2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, and SP 800-219r1, *Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)*, to secure devices and operating systems throughout their life cycles and support zero trust policy, as demonstrated in the NIST NCCoE Zero Trust Architecture (ZTA) project.
- As part of an ongoing study of forensic science, NIST published IR 8354, *Digital Investigation Techniques: A NIST Scientific Foundation Review*.

Learn more about Trustworthy Networks & Platforms priority area

NIST National Cybersecurity Center of Excellence (NCCoE)

Cybersecurity Connections Launch Event

Left to right: Deputy Secretary of Commerce Don Graves, Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio, Maryland Secretary of Commerce Kevin Anderson, and Montgomery County Executive Marc Elrich sign a partnership agreement at the NCCoE.

Credit: Rich Press/NIST

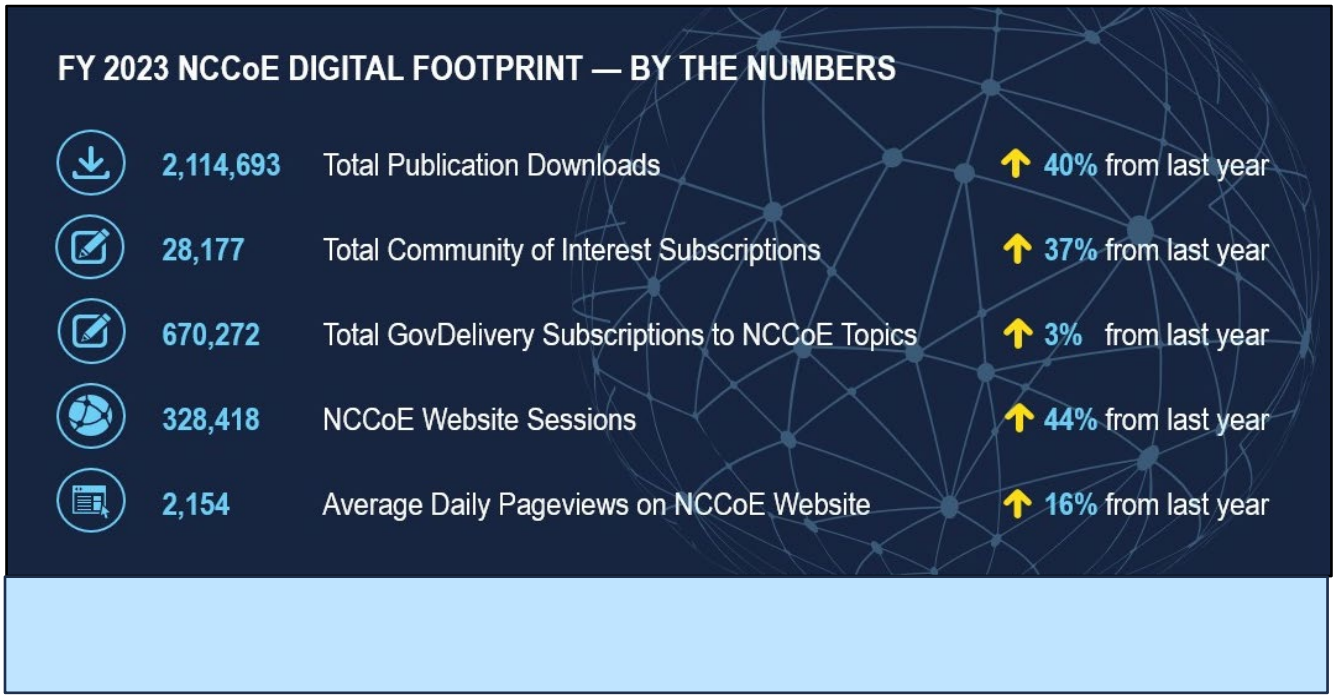
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (NCCoE)

Mission Statement:

"The NCCoE brings 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."

Major Accomplishments in FY 2023:

- **Produced actionable, standards-based guidance.** In FY 2023, the NCCoE released 42 publications. These consisted of draft and final versions of NIST 1800 Series Special Publications, NIST Interagency Reports, and short-form guides on a wide range of topics, such as hybrid satellite networks, mobile device security, Internet of Things (IoT), zero trust architecture, genomic data, and more. View our publications here.
- **Renewed partnership with federal, state, and county governments.** In March 2023, NIST, the Maryland Department of Commerce, and Montgomery County signed a five-year agreement to extend their partnership in support of the NCCoE. According to a press release issued by NIST, "One goal of the renewed partnership agreement is to better address the needs of companies and institutions in the state and county, with a particular focus on small business."
- **Launched Cybersecurity Connections.** NCCoE introduced the Cybersecurity Connections Initiative in March 2023. This initiative offers the regional small business community opportunities to engage with experts at the NCCoE to learn about our work and areas of collaboration. In June 2023, NCCoE hosted its first Cybersecurity Connections event, which focused on mitigating and managing cyber risks in the water and wastewater sector.
- **Appointed a new director.** On July 31, 2023, Cherilyn Pascoe began her tenure as the new director of the NCCoE.



In FY 2023, the NCCoE also focused on:

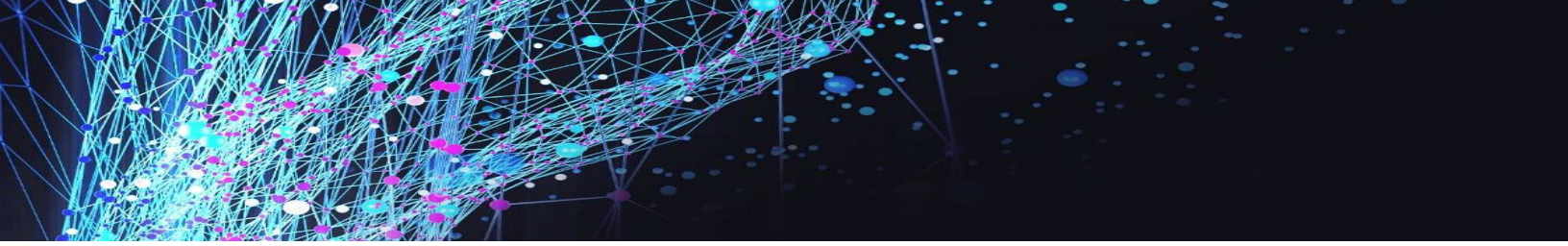
- **Expanding collaborative relationships.** The NCCoE forms long-term collaborative relationships with key stakeholders, primarily through signing Cooperative Research and Development Agreements (CRADAs) with various organizations and Interagency Agreements (IAAs) with government agencies. The NCCoE signed 37 CRADAs this year with 28 tech companies, two government organizations, and two non-profits. The NCCoE also held IIAAs with the Departments of Energy, State, Transportation, and the U.S. Space Force. NCCoE also engages frequently with subject-matter experts and business professionals through our free and publicly available Communities of Interest (COIs). This year, we hosted 29 COIs across sectors and technologies, including a newly launched Small Business COI, to share insights, expertise, and perspectives to guide and increase awareness of our work.
- **Increasing public awareness and understanding.** The NCCoE held 22 events and webinars in FY 2023. We also expanded our video series to provide an inside look at the NCCoE, as well as our healthcare, mobile device, and supply chain assurance labs.
- **Enhancing academic outreach and engagement.** The NCCoE continued its summer internship program for the thirteenth straight year by hosting twelve undergraduate and two graduate students who worked on a variety of projects. This was also the first year that the NCCoE participated in NIST's Summer Institute, which helps provide middle school teachers with cybersecurity resources and tools to shape their curricula.
- **Progressing the Cryptographic Module Validation Program (CMVP) project.** This year, the NCCoE organized an effective governing structure for the community of collaborators to the automation of the CMVP project. NCCoE also published draft SP 1800-40A, *Automation of the NIST Cryptographic Module Validation Program*, which aims to shorten the validation cycle of cryptographic modules for compliance with security standards, while maintaining and improving assurance levels. The team also successfully demonstrated the Phase I prototype at the International Crypto Module Conference (ICMC) 2023.

Learn more about this priority area

OPPORTUNITIES TO ENGAGE WITH NIST ON CYBERSECURITY AND 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.



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

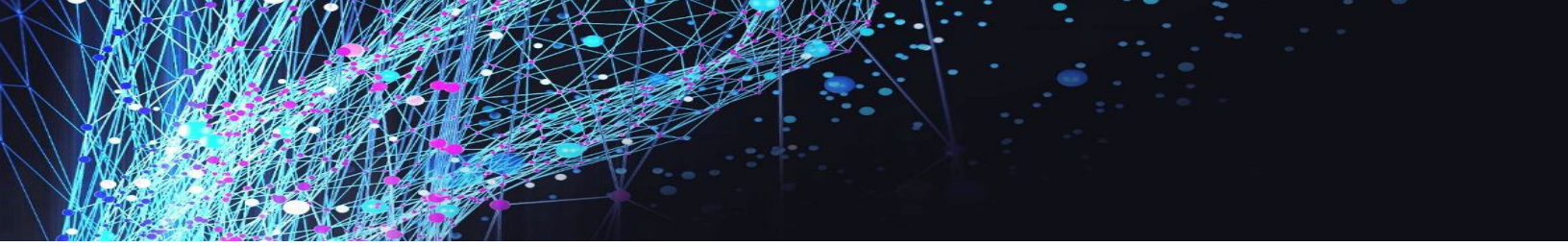
O'Reilly PD, II, Rigopoulos KG (2024) Fiscal Year 2023 Cybersecurity and Privacy Annual Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-229. https://doi.org/10.6028/NIST.SP.800-229

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.

Contact Information

cyber@nist.gov



Abstract

During Fiscal Year 2023 (FY 2023) – from October 1, 2022, through September 30, 2023 –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 2023 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; release of a Phish scale; progress in the Identity and Access Management program; Strategic and Emerging Research Initiatives (SERI) for autonomous vehicles.

Keywords

annual report; 2023 annual report; cybersecurity; cybersecurity program; cybersecurity and privacy program; Federal Information Security Management Act; FISMA; privacy; program highlights; project highlights; information security; Information Technology Laboratory; ITL; program accomplishments; project 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.