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

SPECIAL PUBLICATION 800-238

CYBERSECURITY & PRIVACY PROGRAM ANNUAL REPORT 2025

NIST Special Publication 800
NIST SP 800-238

Fiscal Year 2025 Annual Report for NIST Cybersecurity and Privacy Program

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.800-238

May 2026

U.S. DEPARTMENT OF COMMERCE
Howard Lutnick, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Table of **CONTENTS**

FOREWORD

Julie Chua
Chief, Applied Cybersecurity Division

Jon Boyens
Acting Chief, Computer Security Division

Each year, as we reflect on memories and accomplishments, we are reminded of the enduring legacy and evolution of our work at NIST. This Annual Report is our twenty-third in a row…and a lot has changed throughout the years. One thing that has not wavered is our ability to understand the complex cybersecurity landscape and pivot our research and work accordingly.

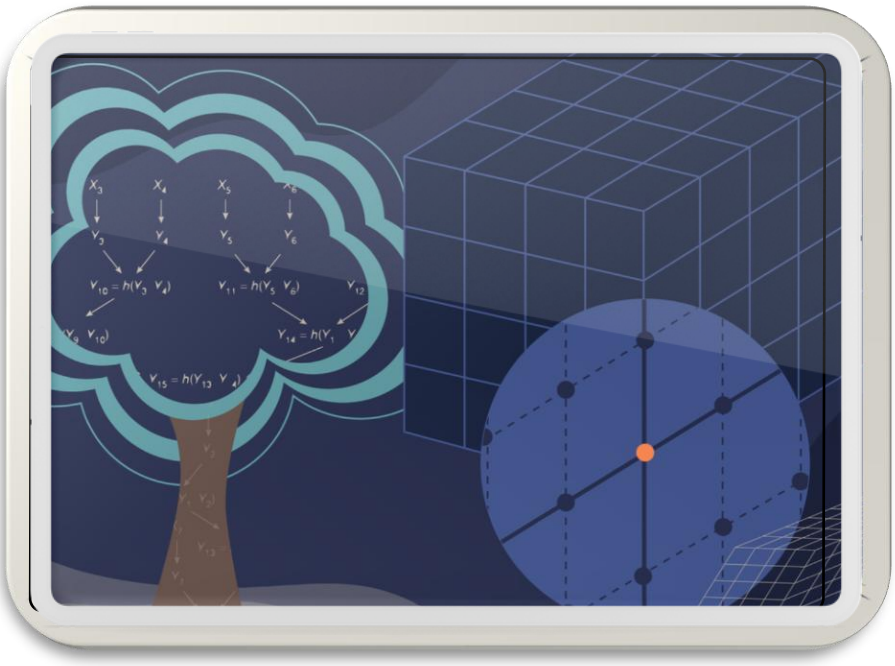
Amid evolving threats, rapid technological advancements, and an increasingly intricate global ecosystem, our cybersecurity and privacy NIST colleagues and external partners, including collaborations at the NIST National Cybersecurity Center of Excellence (NCCoE), accomplished so much this year. They delivered important publications and guidelines, hosted events, fostered critical collaborations, and advanced innovative research that strengthens global cybersecurity, standards, and privacy. Our work cut across disciplines at NIST, including our work in standards, risk management, supply chain, small business, and privacy. These accomplishments are a testament to the unwavering dedication and resilience of our talented teams, partners, and stakeholders.

As we look to the future, we are filled with profound optimism. The foundation we have built positions us not only to address today's challenges, but to anticipate and shape tomorrow's opportunities in cybersecurity and privacy. Thank you for your continued support and engagement with NIST's vital mission.

Julie and Jon

Cryptography

NIST has fostered the development of trustworthy cryptographic techniques and technologies for over 50 years through open, collaborative processes that incorporate input and expertise from industry, government, and academia. Our cryptographic standards, guidelines, and test methods help secure global e-commerce and protect U.S. federal information.



Credit: NIST

Cryptography

FISCAL YEAR 2025

Major accomplishments:

- Continued to advance post-quantum cryptography (PQC) standards by announcing a fifth PQC algorithm for standardization, Hamming Quasi-Cyclic (HQC), and working with industry and standards development organizations to facilitate PQC adoption in critical security technologies.
- Released a timeline for the migration to PQC standards, the deprecation of quantum-vulnerable algorithms after 2030, and the required use of quantum-resistant algorithms by 2035.
- Published the lightweight cryptography standard Ascon in SP 800-232 after a five-year global competition to provide strong, efficient, side-channel-resistant protection for billions of Internet of Things (IoT) and constrained devices for which traditional cryptography is too costly.
- Strengthened trust in the security of commercial cryptographic products through testing under the Cryptographic Module Validation Program with improved workflows and processes to reduce the time for validation for the 262 products tested in FY 2025.
- Expanded collaboration on the Migration to PQC Project, with 50+ organizations working to demonstrate practices to ease migration to NIST PQC standards. This included demonstrations of the functionality of some collaborator discovery and inventory tools (and how the tool outputs could be used to prioritize migration decisions). Collaborators also demonstrated the interoperability of PQC algorithms to prepare for their use in products and services. (NCCoE)
- Expanded automated cryptographic algorithm testing to deliver nearly 1 million test vectors and validate 1,598 implementations while facilitating the migration to PQC standards with 170 Module-Lattice-Based Digital Signature Algorithm (ML-DSA) (from FIPS 204) and Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) (from FIPS 203) validations.

Learn More

Cybersecurity & AI

Artificial intelligence (AI) systems are being used and deployed on an increasing number of tasks, including processing and analyzing large quantities of data. AI systems introduce new opportunities and potential security concerns. This focus area explores the management of risks to people and organizations who use AI systems.

Credit: Shutterstock

Cybersecurity & AI

FISCAL YEAR 2025

Major accomplishments:

- Published a concept paper and generated critical input for the Cybersecurity Framework Profile for AI through a workshop and multiple working meetings involving thousands of participants. (NCCoE)
- Released *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, which is widely cited and discussed.
- Collected real-world data from experiments on a 'smart road' to accelerate the development of new-generation benchmark datasets to help improve the robustness of AI models used in self-driving cars. (NCCoE)
- Kicked off the Control Overlays for Securing AI Systems (COSAiS) project to develop a series of overlays for securing AI systems using NIST's SP 800-53 controls, SP 800-218A, Draft AI 800-1, and AI 100-2e2025 to facilitate the responsible and secure adoption of AI technologies.
- Published an Institute of Electrical and Electronics Engineers (IEEE) Computer article describing a unified measurement and visualization framework that quantitatively characterizes the strength, weakness, transferability, and explainability of machine-learning training and testing datasets.
- Published findings about a model-agnostic dataset reduction method using Combinatorial Frequency Differencing to identify distinguishing feature values at a peer-reviewed conference.
- Published a paper in the Association for Computing Machinery Workshop on Computer Security on threat modeling for security analysis of machine learning systems.
- Published a paper on detecting hallucinations in a Conference on Data and Applications Security and Privacy proceedings, winning a "Best Paper Award."
- Published a paper on automated program repair in *IEEE Computer*.
- Continued to develop and improve Dioptra, a software test platform for assessing various characteristics of AI systems. (NCCoE)

Learn More

Education & Workforce

The Education and Workforce focus area coordinates programs across sectors to grow and sustain a skilled cybersecurity workforce. This work also includes increasing public awareness of cybersecurity, cybersafety, and cyberethics and disseminating cybersecurity technical standards and best practices for individuals and enterprises.

Credit: Felicia Rateliff

Education & Workforce

FISCAL YEAR 2025

Major accomplishments:

- NICE's Community Coordinating Council released three new resources in support of the NICE Strategic Plan: a white paper on Empowering Organizations to Retain Skilled Cybersecurity Talent for Long-Term Success, information on Options for Entering the Cybersecurity Workforce, and information on Help Wanted: Cybersecurity Educators - How National Centers of Academic Excellence are Responding.
- Released additional resources in support of the NICE Strategic Plan, including information on Skills-Based Approaches to Cybersecurity Talent Management, Unlocking Cybersecurity Talent: The Power of Apprenticeships, and The Impact of Artificial Intelligence on the Cybersecurity Workforce.
- The Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development Program awarded 17 new cooperative agreements totaling over $3 million aimed at building the workforce needed to safeguard enterprises from cybersecurity risks. As of September 2025, NIST has funded 47 RAMPS communities established across 25 states.
- Several events were held throughout FY 2025, including the NICE Conference & Expo, NICE K12 Cybersecurity Education Conference, Regional Initiative for Cybersecurity Education and Training (RICET), Cybersecurity Career Week, NICE webinars, and the US Cyber Team Draft Day.
- NIST continued to support Federal Information Security Educators (FISSEA) engagement throughout FY 2025, including winter, spring, and fall forums.

Learn More

Hardware & Software Security

Computing hardware and software are the building blocks of modern electronics and information systems. The Hardware Security and Software Security programs at NIST are dedicated to developing the standards, guidelines, and best practices that underpin the security and trustworthiness of these systems. Their work focuses on ensuring the integrity of hardware components and the security of software systems, components, and services throughout the development life cycle.

Credit: Shutterstock

Hardware & Software Security

FISCAL YEAR 2025

Major accomplishments:

- Established a Hardware Security Laboratory to enhance semiconductor security through measurements and metrics, including an electrical probing station, electromagnetic side-channel analysis equipment, test artifacts, and initiating experiment development.
- Held a workshop with industry, government, and academia to identify priorities, challenges, and solutions for semiconductor supply chain trust and provenance. Panel discussions and breakouts assessed concerns, approaches, verification needs, and collaboration barriers and outlined actions for a shared roadmap.
- Gathered feedback during a workshop for the Semiconductor Manufacturing Profile and released Draft IR 8546 to establish Cybersecurity Framework (CSF) 2.0–aligned guidelines for enhancing security in semiconductor manufacturing.
- Led the development of advanced security measurement techniques and analytical frameworks that evaluate hardware security failure scenarios, quantify vulnerabilities, assess collusion-based supply chain threats, and determine benchmark mitigation effectiveness for semiconductor devices.
- Demonstrated emerging attack surfaces through multimodel probing of advanced packaging, vulnerability metrics, and defense strategies in the article, "Toward Standardized Vulnerability Assessment of Advanced Packaging Against Probing Attacks" in IEEE's Design & Test issue.
- Launched the Secure Software Development, Security, and Operations (DevSecOps) Practices Project, established an industry consortium to improve secure software development, and published a preliminary draft of SP 1800-44A. (NCCoE)
- The National Checklist Program added ~216 new and updated automated checklists for securely configuring and patching common applications and operating systems used by organizations to secure millions of computer systems.

Learn More

Infrastructure Security

NIST's infrastructure security portfolio delivers relevant guidelines, standards, and technical leadership to strengthen the security of resources and platforms that underpin information technology systems. Through coordinated research, industry collaboration, and contributions to global standards bodies, the program identifies emerging risks, develops practical and risk-based cybersecurity approaches, and supports secure technology adoption across critical sectors.

Credit: Shutterstock

Infrastructure Security

FISCAL YEAR 2025

Major accomplishments:

- Published *Guidelines for API Protection for Cloud-Native Systems* and *Service Mesh Proxy Models for Cloud-Native Applications*, which recommend practical security controls and a risk-based approach to API protection.
- Published the *CSF 2.0 Manufacturing Profile*, which provides a voluntary, risk-based approach for managing activities and reducing cyber risks. (NCCoE)
- The 5G Cybersecurity project published several white papers on potential concerns and mitigations for 5G systems: CSWP 36C, CSWP 36D, and CSWP 36E. (NCCoE)
- The High-Performance Computing (HPC) Security Working Group released SP 800-223 and Draft SP 800-234 to enhance communication on HPC security, facilitate security compliance, and enable guided system designs globally.
- Updated Draft IR 8259 (Rev 1), which recommends cybersecurity activities for manufacturers. (NCCoE)
- The Cybersecurity for the Manufacturing Sector Consortium project is currently under review. (NCCoE)
- Participated in the third-generation partnership project (3GPP) SA3 to ensure appropriate input into cybersecurity for cellular standards, including the use of NIST Cryptographic Algorithm standards in 5G and 6G cellular networks.
- The Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management project hosted an open house for collaborating organizations to demonstrate their solutions. (NCCoE)
- Convened bi-monthly Cooperative Research and Development Agreement partner meetings to engage with water sector stakeholders, present findings at conferences and meetings, and establish NIST's role as an advocate for cybersecurity best practices in the water sector. (NCCoE)

Learn More

Risk Management

The Cybersecurity and Privacy Risk Management portfolio encompasses research, standards, and frameworks that enable the understanding, assessment, measurement, management, and communication of risks from the component to the enterprise level. These efforts serve as the foundation for the entire NIST Cybersecurity and Privacy program.

Credit: Shutterstock

Risk Management

FISCAL YEAR 2025

Major accomplishments:

- Advanced the adoption of the Cybersecurity Framework 2.0 (CSF 2.0) by releasing quick-start guides, adding informative references to the CSF 2.0 Tool in the Online Informative References, launching a Webinar Series, publishing translations of resources, and updating the NIST IR 8286 series.
- Published 7 community profiles and resources across sectors. (NCCoE)
- Released SP 800-55 Vols. 1 and 2 on identifying and selecting security measures and developing an information security measurement program.
- Updated the enhanced security requirements for protecting CUI and assessment procedures and issued a small business primer.
- In response to Executive Order (EO) 14306, issued updates to the Security and Privacy Control Catalog (SP 800-53 Release 5.2.0) and Assessment Procedures (SP 800-53A Release 5.2.0) for secure and reliable software updates and patches.
- Drove the adoption of Cybersecurity Supply Chain Risk Management best practices by leading the Software and Supply Chain Assurance Forum and supporting the Federal Acquisition Security Council.
- Published draft Privacy Framework 1.1, which received 250+ comments from 31 stakeholders and was downloaded 25,000+ times.
- The Open Security Controls Assessment Language (OSCAL) continued to increase security program automation. The CAPORDINO tool was released, which converts reference datasets managed by the Cybersecurity and Privacy Reference Tool into OSCAL formats.
- Released Revision 4 of the *Digital Identity Guidelines*, delivered resources on Mobile Driver's Licenses for opening accounts and high-risk transactions, contributed to ISO/IEC TS 18013-7:2025 (an international, interoperable protocol to securely present important identity documents), and developed a reference implementation of an International Organization for Standardization (ISO) standard. (NCCoE)
- NICE Workforce Framework Version 2.2.0 was issued, featuring a new Operational Technology Cybersecurity Engineering Work Role.

Learn More

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 (2025) Fiscal Year 2025 Annual Report for NIST Cybersecurity and Privacy Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-238. https://doi.org/10.6028/NIST.SP.800-238

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

Throughout Fiscal Year 2025 (FY 2025) — from October 1, 2024, through September 30, 2025 — 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 ITL Cybersecurity and Privacy Program's FY 2025 research activities, including the ongoing participation and development of international standards, research, and practical applications in several key priority, including improved software and supply chain cybersecurity, work on IoT cybersecurity guidelines, National Cybersecurity Center of Excellence (NCCoE) projects, a new comment site for NIST's Risk Management Framework, the release of a Phish scale, and progress in the Identity and Access Management program.

Keywords

annual report; 2025 annual report; cybersecurity; cybersecurity program; cybersecurity and privacy program; Federal Information Security Modernization Act; FISMA; information security; Information Technology Laboratory; ITL; privacy; program accomplishments; program highlights; project accomplishments; project highlights.

Reports on Computer Systems Technology

The ITL at 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 | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE