

2020

Cybersecurity and Privacy Annual Report



2020 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
Annapolis Junction, Maryland

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
<https://doi.org/10.6028/NIST.SP.800-214>

SEPTEMBER 2021



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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Table of Contents

Foreword.....	1
Focus Area 1: Cybersecurity Awareness and Education	2
Focus Area 2: Identity and Access Management.....	4
Focus Area 3: Metrics and Measurement.....	7
Focus Area 4: Risk Management	10
Focus Area 5: Privacy Engineering	14
Focus Area 6: Emerging Technologies.....	16
Focus Area 7: Cryptographic Standards and Validation	19
Focus Area 8: Trustworthy Networks	23
Focus Area 9: Trustworthy Platforms	27
ITL Leadership and Participation in National and International Standards Programs.....	30
Opportunities to Engage with the NIST Cybersecurity & Privacy Program.....	31

Foreword



With each day bringing new cybersecurity and privacy challenges and advances, it is little wonder that many leaders feel as if they have been cast in the role of the Red Queen in Lewis Carroll's "Through the Looking-Glass." In that classic, the Queen tells Alice: "Now, here, you see, it takes all the running you can do to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"

It is true that leaders need to be nimble and move quickly to avoid the consequences of cybersecurity and privacy attacks that threaten their enterprises. That need extends to government agencies, like NIST, that are trying to help meet those urgent challenges.

At NIST, we know that – in addition to current needs – we also have a responsibility to keep an eye on the horizon, anticipating technology changes, threat environments, and cultural shifts that could affect the ability of organizations to manage cybersecurity and privacy risks.

We've successfully carried out our work for nearly 50 years precisely because we not only address near-term challenges but also spend time thinking, exploring, listening, and speaking with others about the really big issues in store for all of us. We tackle current issues, but we also play the long game – the infinite game, if you will. We are mindful of the reality that cybersecurity and privacy challenges are evolving. At NIST, we make it our business to help others be prepared by anticipating needs and creating opportunities. We anchor our decisions with our feet firmly planted in both the present and the future. As you read this report about our efforts and accomplishments in 2020, you will understand how we have been addressing both short-term and long-term needs.

For example, in the cryptographic arena, we are not only providing and improving practical tools and services for today, we also are rapidly moving forward to ensure that Post-Quantum Cryptography standards are ready when quantum computing becomes a real threat to the protective algorithms that we all take for granted. We have been integrating privacy considerations into the basic control suites that so many organizations rely on now, and we are widening our privacy focus to encompass the broader privacy concerns that arise as mobile computing, e-commerce, and the Internet of Things advance. The intentional addition of the word "privacy" in this report's title reflects changing technological capabilities and society's expectations.

This year's annual report is grouped into nine priority areas for NIST, with most – but not all – of the work being conducted by our Information Technology Laboratory (ITL) and in close collaboration with the private and public sectors. While these represent areas that NIST believes merit the bulk of our attention for the foreseeable future, the report also includes other specific projects of importance that do not fit neatly into these buckets.

All of this work adds up to cultivating trust in information, systems, and technologies. That's our charge. That's our reason for being. I encourage you to review our recent progress and to help us look well beyond the here-and-now of technology, cybersecurity, and privacy; this will enable all of us to meet the future with confidence that we can manage the emerging risks and change the world for the better for the next 50 years.

Kevin Stine
NIST Chief Cybersecurity Advisor

1 | Cybersecurity Awareness and Education



Credit: Shutterstock

NIST continues to coordinate a National Cybersecurity Awareness and Education Program that includes activities such as the widespread dissemination of cybersecurity technical standards and best practices; efforts to make cybersecurity best practices usable by a variety of individuals and stakeholders; increasing public awareness of cybersecurity, cyber safety, and cyber ethics; increasing the understanding of the benefits of ensuring effective risk management of information technology and the methods to mitigate and to remediate vulnerabilities; supporting formal cybersecurity education programs at all levels to prepare and improve a skilled cybersecurity workforce; and promoting initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) is a partnership among government, academia, and the private sector. NICE is focused on cybersecurity education, training, and workforce development. NIST's leadership of the program helps position it to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

NICE's mission is to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development. This mission supports the vision of helping to secure the nation by increasing the number of skilled cybersecurity professionals.

In Fiscal Year (FY) 2020, the National Initiative for Cybersecurity Education (NICE) finalized two publications. The first, NIST Interagency or Internal Report (NISTIR) 8287, *A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce*, provides a summary of how to create ecosystems and partnerships to stimulate cybersecurity education and workforce development.

The second, NIST Special Publication (SP) 1500-16, *Improving Veteran Transitions to Civilian Cybersecurity Roles: Workshop Report*, presents the findings and recommendations from a workshop on how to help transitioning military members discover opportunities in the cybersecurity workforce.

NICE also curated a webpage for free and low-cost online cybersecurity learning content. At a time when many are transitioning to remote learning or considering a job or career change, this resource provided links to training courses, labs, and curriculum for the purposes of progressing toward new skills or credentials in cybersecurity.

NICE hosted several events in FY 2020. In addition to monthly webinars, NICE held two annual conferences – the NICE Conference and Expo in Phoenix, Arizona, which had more than 800 registrants; and the NICE K12 Cybersecurity Education Conference in Garden Grove, California, which had more than 450 registrants. NICE also conducted a workshop on Use Cases for the NICE Framework and the annual National Cybersecurity Career Awareness Week where organizations from around the world held virtual and in-person events to help inspire and promote awareness and exploration of cybersecurity careers.

Advancing Cybersecurity Usability

NIST has popularized the “Phish Scale” as a method to better characterize an organization’s phishing risk. The scale considers phishing cues and user context to help Chief Information Security Officers and phishing training implementers rate the difficulty of their organizations’ phishing exercises and explain associated click rates. NIST’s Video and Digital Media Production Group created a video for the Phish Scale, and research results were published in the *Journal of Cybersecurity* and highlighted in a NIST article that garnered media attention across industry, government, and academia.

NIST also completed an in-depth interview study to understand consumers’ challenges, perceptions, and experiences related to smart home security and privacy. The results of the study inform the Internet of Things (IoT) security and privacy guidelines by identifying current gaps in users’ experiences and suggesting how smart home devices might be designed to better integrate usability, privacy, and security. The capstone paper describing the results will be published in the proceedings of the 2021 USENIX Security Symposium.

Small Business Cybersecurity Corner

In FY 2020, the Small Business Cybersecurity Corner website organization and design were updated based on the results of a usability study conducted by a set of small business owners.

In addition to facilitating access to many popular small business security resources, the language of the site was updated to be more accessible and relatable to the small business community. Training materials and accompanying resources continue to be expanded based on cybersecurity resources and feedback received from NIST’s federal partners and the public.

2 | Identity and Access Management



Credit: Shutterstock

Identity and Access Management (IdAM) is a fundamental and critical cybersecurity capability to ensure that the right people have the appropriate access to the proper resources at the right time. To advance the state of identity and access management, NIST:

- Conducts focused research to better understand new and emerging technologies, impacts on existing standards, and ways to implement IdAM solutions;
- Leads in the development of national and international IdAM standards, guidance, best practices, profiles, and frameworks to create an enhanced, interoperable suite of secure, privacy-enhancing solutions;
- Evolves its IdAM standards, guidelines, and resources; and
- Produces example solutions that bring together the IdAM requirements needed to address specific business cybersecurity challenges.

IdAM is an important component of cloud computing security, and NIST publishes access control characteristics and general access control guidelines for various cloud service models. NIST also performs research and development regarding access control rules and methods.

Personal Identity Verification (PIV)

As required by Homeland Security Presidential Directive 12, NIST developed and maintains the Federal Information Processing Standard (FIPS) for personal identity verification (PIV) of federal employees and contractors (FIPS 201). In FY 2019, NIST initiated a revision of FIPS 201 to incorporate changing business requirements of federal departments and agencies and to adapt to an evolving technology environment. The revision also helps users to align with Office of Management and Budget (OMB) Policy Memorandum M-19-17. Revision activities began in FY 2019 with a business requirement meeting to engage with federal stakeholders about the revision goals. In FY 2020, the PIV team updated the draft standard based on the revision goals

and published public draft FIPS 201-3. The draft standard expands the set of PIV authenticators beyond the current practices (including the current smart card form factor) while addressing interagency use of new types of PIV authenticators (i.e., derived PIV credentials) via federation. The revision also aims to facilitate the issuance of PIV cards by enabling remote identity proofing. These changes closely align with M-19-17. For FY 2021, the PIV team will actively work on resolving comments on the public draft while continuing outreach to federal stakeholders.

Digital Identity Guidelines

The four-volume set of NIST SP 800-63-3, *Digital Identity Guidelines*, was published in June 2017. Following three years of federal agency experience implementing the controls and requirements and to help stay ahead of potential online identity attacks, the Information Technology Laboratory (ITL) decided to revise and update all volumes of SP 800-63-3.


NIST ITL published the pre-draft Request for Comments for the revision of SP 800-63-3 on June 8, 2020. The Request for Comments identified nine topics for potential update. Additionally, NIST ITL provided numerous virtual conferences and presentations on the targeted topics for potential revision and other aspects of the Digital Identity Guidelines to improve and focus the development and submission of comments. More than 40 federal agencies and industry organizations responded with over 300 comments. ITL published a public roadmap for key activities, milestones, and target dates for the development of SP 800-63, Revision 4, and published all comments received by the comment closing date. As indicated in the roadmap, ITL plans to complete adjudication of comments received in the first quarter of FY 2021 and will post issues for potential revision on GitHub in the second quarter.

Implementation Resources for NIST SP 800-63, *Digital Identity Guidelines*

In June 2020, NIST ITL published resources for applying NIST SP 800-63. Based on requests from federal agencies and industry and on recommendations from the U.S. General Accountability Office (GAO), NIST developed and published materials to provide non-normative guidance for the implementation of SP 800-63A, *Enrollment and Identity Proofing*; SP 800-63B, *Authentication and Lifecycle Management*; and SP 800-63C, *Federation and Assertions*. The guidance addresses key topics and aspects of each volume to facilitate the understanding and implementation of the requirements for all assurance levels. ITL presented information for federal agencies and industry to promote the use of the implementation resources and discuss key topics, requirements, and controls and how to properly implement them.

Conformance Criteria for NIST SP 800-63A and 800-63B

OMB Policy Memorandum M-19-17 updated federal identity, credentials, and access management policy and provided direction for federal agencies to enhance associated capabilities. The OMB Policy Memo assigned NIST the responsibility for developing conformance criteria for accreditation of products and services to meet the designated levels of assurance in SP 800-63-3. In response, NIST ITL developed the criteria for NIST SPs 800-63A and 800-63B.



The conformance criteria present all normative requirements and controls of SP 800-63-3 by designated assurance level, the control objectives for each criterion, recommended methods for determining conformity, and supplemental guidance to assist implementers and assessors. The criteria are intended for federal agencies and industry service providers for the implementation of SP 800-63-3 and for conducting conformance and security assessments under the Federal Information Security Modernization Act (FISMA). NIST provided virtual conferences and presentations to explain how to apply and use the conformance criteria for implementation and conformance assessment. Multiple federal agencies and industry organizations have developed programs to incorporate the conformance criteria and take advantage of the guidance and tools presented in the document.

Access Control System Guidance and Research for Cloud Systems

NIST developed SP 800-210, General Access Control Guide for Cloud Systems, to present cloud access control characteristics and general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The main focus is on the technical aspects of access control without considering deployment models (e.g., public, private, hybrid clouds). It also focuses on trust and risk management issues, which require different layers of discussions that depend on the security requirements of the business function or the organization of deployment for which the cloud system is implemented. NIST researched emerging technologies that can be applied to access control mechanisms, such as the Natural Language Processing algorithm to automatically generate access control policy from natural language documentation. Currently, studies of experiment tools, user cases, and language features are the focus of the research work.

Access Control Policy Verification and Development Tools

Access control systems are among the most critical network security components. Faulty policies, misconfiguration, or flaws in software implementation can result in serious vulnerabilities. To address these issues, NIST developed and is improving the Access Control Policy Tool (ACPT), which allows a user to compose, verify, test, and generate access control policies. New user-interface features have been added to the improved version of ACPT. NIST has also developed the Access Control Rule Logic Circuit (ACRLC) simulation technique, which enables access control policy authors to detect a fault when the fault-causing access control rule is added to the policy. This notification allows a fix to be implemented in real time before adding other rules that further complicate the detecting effort.

In addition to software simulation, NIST worked on hardware implementation of ACRLC with the University of Arkansas Computer Science Department. The hardware version of ACRLC enables the study of performance and real-world applications. NIST also researched theories for applying quantum algorithms to limited access control systems (such as IoT devices). The research results are presented in the paper Apply Quantum Search to the Safety Check for Mono Operational Attribute Based Protection Systems, which will be published in the international Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage.

3 | Metrics and Measurement




Credit: Shutterstock

Cybersecurity Metrics provide decision support, and they help to measure and improve performance and accountability for cybersecurity activities. A mature metrics program is content-rich, supports a broader range of stakeholders, and provides greater value to the organization. More precise measurement data helps to focus on an actionable approach to improving cybersecurity. To support this effort, NIST has embarked on various initiatives, some of which are highlighted here. Initiatives include research in new technology areas, risk management tools and guidance, and ways for organizations to mature the use of cybersecurity metrics.

Measurements for Information Security

Every organization wants to gain maximum value and effect for its finite cybersecurity-related investments. This includes managing risk to the enterprise and optimizing the potential reward of cybersecurity policies, programs, and actions. Organizations frequently make decisions by comparing scenarios of various projected costs with potential associated benefits and risk reduction. Senior executives need accurate and quantitative methods to portray and assess these factors, their effectiveness and efficiency, and their effect on risk exposure. Providing reliable answers to these questions requires organizations to employ a systematic approach to cybersecurity measurement that considers current knowledge limits.

NIST's cybersecurity measurements program enables organizations to manage cybersecurity risks. NIST is undertaking a focused program on cybersecurity measurements to support the development and alignment of technical measures to determine the effect of cybersecurity risks and responses on an organization's objectives. The initiative involves collaboration with the research, business, and government sectors.



In FY 2020, NIST issued a request for public comments on NIST SP 800-55, Revision 1, *Performance Measurement Guide for Information Security*. NIST also created a website to aggregate guidelines, tools, research, and resources for improving the quality and utility of information to support decision making.

Cyber Risk Analytics

This project promotes technical solutions that enable organizations to bridge new and existing data sets to advance cyber risk analysis and enhance the ability to report trends. The goal is to facilitate information sharing among risk owners about historical, current, and future cyber risk conditions. NIST is leveraging past and present efforts such as using a data repository for cyber incident analysis, predictive analytics and strategic analysis on threat coverage, and prioritization and gap identification. In FY 2020, research involved developing a proof-of-concept sandbox for a trusted and secure repository in which enterprise risk owners can anonymously share, store, aggregate, and analyze cyber incident data. As such, initial efforts explore the enabling of capabilities such as anonymization, provenance, data enrichment, and data quality. NIST will continue to explore data analytics to improve the understanding of cybersecurity risks and inform management practices.

Additional software assurance projects included:

- Software Assurance Metrics and Tool Evaluation (SAMATE) improves software assurance by developing methods to enable software tool evaluation, measure the effectiveness of tools and techniques, and identify gaps in tools and methods.
- The Bugs Framework (BF) provides precise definitions of software bugs and language-independent taxonomies for describing software vulnerabilities. In FY 2020, BF published models and definitions.
- Software Assurance Reference Dataset (SARD) is a large collection of programs that contain known software flaws. In FY 2020, NIST enhanced SARD with a large collection of test cases contributed by the National Security Agency's Center for Assured Software.
- Static Analysis Tool Exposition (SATE) advances research in static analysis tools to find security-relevant source code weaknesses. NIST provides reference test cases to software assessment product vendors, and those vendors return the results of their products' analyses to NIST to help better understand how to identify and report software weaknesses.

Automated Combinatorial Testing

Automated Combinatorial Testing (ACT) research focused on the application of combinatorial methods for assurance of artificial intelligence (AI) and machine learning (ML) systems. ACT developed a new method and tool for analyzing and explaining the decisions of AI/ML algorithms, presented this research to U.S. Air Force and U.S. Army researchers, and collaborated with Virginia Tech on autonomous systems assurance.

Computer Forensic Tool Testing

Computer Forensic Tool Testing (CFTT) is supported by the NIST Special Programs Office and the Department of Homeland Security (DHS). In FY 2020, several key advances were made to help address a critical need in the law enforcement community to ensure the reliability of computer forensic tools. CFTT tested the attributes of numerous digital forensic tools, and federated testing was developed to provide third parties with the ability to use the NIST testing methodology in their own labs and produce standardized test reports. In FY 2020, NIST upgraded the core infrastructure and added 14 published reports.

Computer Forensic Reference Data Sets

Computer Forensic Reference Data Sets (CFReDS) is a repository of documented sets of digital evidence. In FY 2020, the development of an improved portal began. The goal is for the CFReDS website to be a centralized portal for the forensic community to find and share datasets of interest. The Forensics Tool Catalog is a web-based, community-sourced catalog of tools aided by a taxonomy.

National Software Reference Library

The National Software Reference Library (NSRL) collects software from various sources and incorporates file profiles into a Reference Data Set (RDS) of information. The RDS can be used by members of law enforcement, government, and industry to review computer files by matching file profiles in the RDS. This helps alleviate the effort involved in determining which files are important as evidence on computers or file systems seized as part of criminal investigations. NSRL provides a research environment to promote the development of new forensic techniques and other applications in computer science. In FY 2020, the NSRL published four releases of software metadata and enlarged the collection to a combined total of 798 million files.

4 | Risk Management



Credit: Shutterstock

Throughout FY 2020, NIST has made significant progress in advancing methods and guidelines for managing enterprise risk related to cybersecurity, systems engineering, and privacy. NIST is leading a multi-year effort to produce a cohesive portfolio of complementary risk management resources that can be used individually or together to help public and private organizations better manage cybersecurity and privacy risk at all levels of the enterprise.

Risk management has been a fundamental driver for organizations for as long as there has been information to protect. Today's proliferation of risk management resources, combined with advances in technology, increasingly call for a collaborative approach to managing discipline-specific risks within the enterprise. This includes the need to ensure that managers, risk professionals, developers, and designers work together to implement secure engineering practices. These practices will help to ensure more secure systems, including those managed by external partners, and expanded risk management applications for an evolving range of products.

Risk Management Framework Updates

The Risk Management Framework (RMF) is one of NIST's most popular and widely used products. Initially created for federal agencies, organizations around the globe use the RMF because it provides a structured and flexible process for managing security and privacy risk.

In FY 2020, NIST published SP 800–53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, which is the first and only comprehensive catalog of information security and privacy countermeasures that provide a foundation for protecting organizations, systems, and the personal privacy of individuals. The update represents a multi-year effort that supports a proactive and systematic approach to ensuring that critical systems, components, and

services are sufficiently trustworthy and have the necessary resilience to support organizational missions. To this end, NIST has supported public and private-sector outreach for interested stakeholders, including hosting a virtual event with over 8,500 participants.

The most significant changes to SP 800-53, Revision 5, include:

- Making controls outcome-based
- Consolidating the control catalog to address information security, privacy, and supply chain risk management
- Adding state-of-the-practice controls to support cyber resiliency, secure systems design, security and privacy governance, and accountability
- Transferring control baselines, including the first federal privacy control baseline, and tailoring guidance to a separate publication, NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*

Supporting the Implementation of the RMF and SP 800-53

NIST continues to develop publications that support the implementation of the RMF steps, including Volume 4 in the NISTIR 8011 series, *Automation Support for Security Control Assessments: Software Vulnerability Management*. NISTIR 8011, Volume 4, addresses the automation of security control assessment, helping with the software vulnerability management of security capabilities and facilitating the risk management of defects that are present in software on the network.

NIST also published SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*. NIST SP 800-137A details an approach for the development and evaluation of Information Security Continuous Monitoring (ISCM) programs. An ISCM program assessment provides organizational leadership with information about the effectiveness and completeness of the organization's continuous monitoring program, including the review of ISCM strategies, policies, procedures, operations, and the analysis of continuous monitoring data.

Integration of Cybersecurity Risk Management into Enterprise Risk Management

The increasing frequency, creativity, and severity of cybersecurity attacks mean that all enterprises should ensure that cybersecurity risk is receiving appropriate attention within their enterprise risk management (ERM) programs. In FY 2020, NIST developed NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management*, to help enterprise stakeholders improve and apply the use of cybersecurity risk management (CSRM) information as an input to ERM processes. By doing so, enterprises and their component organizations can better identify, assess, and manage cybersecurity risks in the context of their broader mission and business objectives. The publication describes the use of risk registers to document, aggregate, and communicate risk elements. Doing so ensures that CSRM is an integral part of ERM, both taking its direction from ERM and informing it.

Advancing the Application of the NIST Cybersecurity Framework

NIST has continued to foster the adoption and application of the NIST Cybersecurity Framework Version 1.1 (the *Framework for Improving Critical Infrastructure Cybersecurity*). The NIST Cybersecurity Framework website has been expanded to provide learning materials, success stories, and other helpful resources. Notably, the team has made significant progress in encouraging global use of the framework and interoperability with other cybersecurity models. Progress includes translation of the framework into several additional languages, including Arabic, Bulgarian, Japanese, Polish, Portuguese, and Spanish. NIST also continues to contribute to international standards development efforts related to cybersecurity risk management and the development of cybersecurity frameworks, including the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) Technical Specification 27110:2021, *Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines*, which is expected to be published in 2021. NIST will also discuss and share information on the Cybersecurity Framework in bilateral and multilateral international dialogues.

A key example of such an application is the development of NISTIR 8323, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*. This publication describes a flexible and voluntary model (based on the Cybersecurity Framework Profile concept) that can be used as part of a risk management program to help organizations manage risks to systems, networks, and assets that use PNT services. The project was launched in support of Executive Order 13905 to help manage risks to PNT signals and data, which are susceptible to disruptions and manipulations that can be natural, manufactured, intentional, or unintentional. Because the Cybersecurity Framework provides a common set of terms and methods for organizing and communicating about risks, such Profiles help foster discussions regarding how to identify important elements, protect against known risks, detect incidents efficiently, and respond and recover effectively in support of critical mission objectives.

In FY 2020, NIST continued to develop the National Cybersecurity Online Informative References (OLIR) Program, an effort to facilitate subject-matter experts in defining standardized reference documents regarding the relationships between elements of their documents and elements of other documents like the NIST Cybersecurity Framework, NIST Privacy Framework, and SP 800-53. While organizations have published written comparisons of various elements (e.g., between NIST SP 800-53 controls and the Cybersecurity Framework Subcategories) for many years, the OLIR Program provides a standardized format for digitally expressing those relationships. To support consistent usage, NIST developed NISTIR 8278A, *National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers*. The OLIR Program can incorporate any authoritative documents, from national and international standards, guidelines, frameworks, and regulations to policies for individual organizations, sectors, and jurisdictions. Cybersecurity document owners can use the OLIR Program as a mechanism for communicating with owners and users of other cybersecurity documents.

Cyber Supply Chain Risk Management

NIST continued work on the Cyber Supply Chain Risk Management (C-SCRM) program. C-SCRM is the process of identifying, assessing, and responding to risks associated with the distributed and interconnected nature of information, communications, and operational technology product and service supply chains. C-SCRM is integrated into Systems Security Engineering (SSE) and covers the entire system life cycle (including research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal) since supply chain threats and vulnerabilities may (intentionally or unintentionally) compromise a technology product or service at any stage.

C-SCRM work in FY 2020 included the following:

- NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks*, describes a prototype solution for filling the gap between an organization's risk appetite and supply chain risk posture by providing a basic measurement of the potential impact of a cyber supply chain event. This tool does not represent a complete C-SCRM solution but is intended to be integrated into or used in concert with tools such as third-party management, enterprise resource planning, and supply chain management.
- The Federal Acquisition Security Council, which was created as a requirement of the U.S. Federal Acquisition Supply Chain Security Act of 2018, helps develop policies and processes for agencies to use when purchasing technology products. It recommends C-SCRM standards, guidelines, and practices that NIST should develop.
- The Initial Public Draft of NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, provides a high-level summary of practices deemed by subject matter experts to be foundational to an effective C-SCRM program. It is based on an analysis of interviews with companies over several years (leading to the development of 24 case studies), prior NIST research in C-SCRM, and several standards and industry best practices documents. This work builds on the Roadmap for Improving Critical Infrastructure Cybersecurity, a companion document to the NIST Cybersecurity Framework. The NISTIR is based on an analysis of interviews with companies over several years (leading to the development of 24 case studies), prior NIST research in cyber supply chain risk management, and several standards and industry best practices documents.
- Since NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, was published in 2015, many aspects of the laws, regulations, tools, technologies, and practices that encompass the information, communications, and operational technology supply chain risk management (SCRM) ecosystem have changed. NIST has initiated an update of SP 800-161 to incorporate lessons learned over the past several years, updates to relevant NIST guidance, and evolving security and privacy priorities.
- A National Cybersecurity Center of Excellence (NCCoE) demonstration project identified methods by which organizations can verify that their purchased computing devices are genuine and have not been altered.

5 | Privacy Engineering



Credit: Shutterstock

The Privacy Engineering Program (PEP) works to provide trusted, rigorous tools and resources that support innovation and privacy. PEP facilitates dialogues among stakeholders about privacy risk management and promotes an organizational shift away from checklist-based legal compliance to improve privacy measures. The following activities reflect progress made in FY 2020 toward three strategic PEP objectives: advancing the development of privacy engineering and risk management guidelines and resources, positioning NIST as a leader in privacy research, and advancing the development and deployment of privacy-enhancing technologies.

Privacy as a programmatic area intersects with each of the other priority focus areas, making coordination and ongoing engagement critical across a range of technical domains. To advance its strategic objectives, PEP collaborates with other NIST programs including the NCCoE, the Cryptography Group, the FISMA program, and the Cybersecurity for IoT program, as reflected in activities throughout this report.

Privacy Framework

In January 2020, NIST released the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework)*. The Privacy Framework is a voluntary tool to help organizations identify and manage privacy risks. This helps them provide innovative products and services while protecting individuals' privacy. Since its release, organizations have adopted the Privacy Framework to improve privacy programs, drive alignment and collaboration with security programs, and more effectively communicate about privacy risk management and resource allocation with their leadership.

To support organizations' use of the Privacy Framework, NIST launched an online, community-driven Privacy Framework Resource Repository for collecting and sharing crosswalks, common Profiles, guidelines, and tools that now contains more than forty resources. NIST also published a

companion roadmap to the Privacy Framework, highlighting priority areas that pose challenges to organizations in achieving their privacy objectives. This document supports continued collaboration between NIST and stakeholders from government, academia, and industry.

Workforce Advancement

As recognized in the Privacy Framework companion roadmap, stakeholders have signaled that demand for a robust and effective privacy workforce is outpacing supply. To support the development of a workforce capable of managing privacy risk and provide a common language around roles, tasks, knowledge, and skills, NIST initiated the development of a privacy workforce taxonomy aligned with the Privacy Framework and the NICE Workforce Framework. NIST launched this effort by collecting stakeholder feedback during the International Association of Privacy Professionals (IAPP) virtual event, “Help Wanted: Growing a Workforce Capable of Managing Privacy Risk.” The working sessions were attended by participants representing a broad spectrum of the public and private sectors, including consulting, consumer technology, energy, financial, non-profit, transportation, law, manufacturing, academia, and standards organizations. NIST will use the stakeholder feedback received at the workshop to inform the development of sets of tasks, knowledge, and skill statements for a privacy workforce taxonomy.

Privacy Leadership

Through leadership positions in key privacy and security organizations, NIST helps drive change and standardization of privacy considerations. NIST personnel co-chaired the Interagency Working Group (IWG) for Privacy with the U.S. Networking and Information Technology Research and Development (NITRD) Program, and served as the first privacy co-chair of the Federal Computer Security Managers’ Forum (FCSM). Through these and many other roles, NIST drives application standards for important risk management focus areas.

Differential Privacy

De-identification techniques can be useful to organizations in mitigating privacy risks. While guidance, standards, practices, and tools are beginning to be developed in this area, more work is needed to increase their market-readiness and assist organizations with implementation. In FY 2020, NIST launched a series of blogs on differential privacy, covering the basics, applicable use cases, and open-source tools available for implementation to leverage the differential privacy contributions indexed in the Privacy Engineering Collaboration Space. The series is designed to help business process owners and privacy program personnel understand basic concepts about differential privacy and applicable use cases and to help privacy engineers and IT professionals implement the tools. NIST’s longer-term goal is to develop a guideline for deploying differential privacy, informed by feedback and engagement generated by the series of blogs.

Leadership and Participation in Developing National and International Standards

During FY 2020, NIST actively engaged with international standards development organizations to advance the development of risk-based standards to help organizations protect individuals’ privacy. NIST participated in the International Organization for Standardization (ISO) Project Committee 317, which focuses on developing ISO 31700, Consumer protection: privacy by design for consumer goods and services; ISO/IEC 27557, Organizational privacy risk management; and Institute of Electrical and Electronics Engineers (IEEE) P7002, Data Privacy Process. In FY 2021, NIST will continue supporting these efforts with a longer-term goal of developing more technical privacy standards in the future.

6 | Emerging Technologies



Credit: Shutterstock

NIST has maintained a long-standing commitment to advancing innovation and supporting cybersecurity and privacy research in emerging technologies and priorities, such as AI, the Internet of Things (IoT), and cloud-native applications based on microservices architecture. NIST's dedicated technical staff, one-of-a-kind facilities, and trusted, objective, non-regulatory role position it well to help the Nation and its partners advance in these promising areas.

Cybersecurity for the Internet of Things (IoT)

NIST's Cybersecurity for IoT program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Accomplishments in FY 2020 included development of the following publications:

- NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers*, recommends six foundational cybersecurity activities that manufacturers can perform to produce more secure devices during the pre-market and post-market product phases. These activities also provide the technical means for customers to secure their own devices, thereby lessening the prevalence and severity of IoT device compromises.
- NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*, identifies a core baseline of technical cybersecurity capabilities for manufacturers to support the protection of an organization's devices, data, systems, and ecosystems across a broad set of use cases.
- NIST posted an online catalog of device cybersecurity capabilities and supporting non-technical manufacturer capabilities that are needed for applying NIST SP 800-53 controls in the federal environment. The catalog takes advantage of GitHub's "issues" feature to provide a highly accessible means for the community to provide feedback.

- NISTIR 8267, *Security Review of Consumer Home Internet of Things (IoT) Devices*, reviewed a number of typical home consumer IoT devices to better understand common security architectures and the typical range of core baseline capabilities in consumer IoT devices.

The IoT program is committed to international engagement. The harmonization of market requirements is critical to improving IoT device security. Cyberthreats do not stop at borders, and market fragmentation does not help improve security. Through ongoing participation in ISO/IEC working groups, NIST has supported the development of international standards that promote security and privacy in IoT devices including:

- Provision of NISTIR 8259 as input to the first draft of ISO/IEC 27402 – *Cybersecurity – IoT security and privacy – Device baseline requirements*; NIST provided comments and participated in working meetings for subsequent drafts.
- Provision of comments and participation in working meetings for ISO/IEC 27400 – *Cybersecurity – IoT security and privacy – Guidelines*.
- Promotion of U.S. interests and strategies on IoT security through participation in the ad hoc working group on IoT Security Standardization.

The IoT program participated in bilateral and multilateral discussions with international governments and industries to increase awareness and utilization of NIST IoT cybersecurity resources. The IoT program engaged with a number of countries and partners across several regions, including Canada, the United Kingdom, Australia, New Zealand, Germany, Taiwan, Japan, the European Commission, and others.

In addition to the publications listed above, the Cybersecurity for IoT program engaged the global community in many ways, including blog posts, webinars, an RSA Conference event, a virtual workshop around the development of a federal profile of the online catalog of capabilities, and a virtual workshop on the risks associated with consumer home IoT devices.

Blockchain Security

Blockchains are tamper-evident and tamper-resistant digital ledgers that are implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community such that under normal operation of the blockchain network, no transaction can be changed once published.

NIST continued its research and development in the use, application, standardization, and interoperability of blockchains and the potential they bring to cultivating trust. In FY 2020, NIST expanded publications and research in some of the following areas:

- NISTIR 8301, *Blockchain Networks: Token Design and Management Overview*
- The use of aggregating atomic clocks for time stamping
- NIST White Paper, *On the Profitability of Selfish Mining Against Multiple Difficulty Adjustment Algorithms*
- NIST White Paper, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*
- Conference Paper, *Implementing a Protocol Native Managed Cryptocurrency*

Artificial Intelligence

NIST contributes to the research, standards, evaluation, and data required to advance the development, use, and governance of trustworthy artificial intelligence (AI). NIST aims to cultivate trust in the design, development, and use of AI technologies and systems by improving measurement science, technology, standards, and related tools in ways that enhance economic security and improve the quality of life.

AI and machine learning (ML) are already changing the ways in which society addresses economic and national security challenges and opportunities, and these technologies must be developed and used in a trustworthy and responsible manner. Characteristics that support trustworthiness include accuracy, explainability, interpretability, reliability, privacy, robustness, safety, security (resilience), and the mitigation of harmful bias. Principles such as transparency, fairness, and accountability should be considered, especially during deployment and use. Trustworthy data, standards, evaluation, validation, and verification are critical for the successful deployment of new technologies for genomics, image and video processing, materials, natural language processing, robotics, wireless spectrum monitoring, and more.

Delivering the needed measurements, standards, and other tools is a primary focus of NIST's portfolio of AI efforts. It is an area in which the agency has special responsibilities and expertise and for which others often turn to NIST for guidance. The agency's AI goals and activities are prioritized and informed by its statutory mandates, White House directives, and the needs expressed by U.S. industry, other federal agencies, and the global AI research community.

NIST's continued AI work is aligned with five broad goals:

1. Conduct fundamental research to advance trustworthy AI technologies.
2. Apply AI research and innovation across the NIST Laboratory Programs.
3. Establish benchmarks and develop data and metrics to evaluate AI technologies.
4. Lead and participate in the development of technical AI standards.
5. Contribute to discussions and development of AI policies.

NIST will continue to collaborate with commercial, academic, and public-sector partners to pursue these goals and collectively advance the security and trustworthiness of this important and emerging technology.

7 | Cryptographic Standards and Validation



Credit: Shutterstock

Network and data security are essential in today's environment of increasingly open and interconnected systems, networks, and mobile devices. Cryptographic standards, algorithms, and methods for encryption, key establishment, and digital signatures provide a critical foundation for mobile device conversations, secure e-commerce transactions, electronic lock access, and much more. Cryptography is a continually evolving field that drives research and innovation. The Data Encryption Standard (DES) was groundbreaking but would fall far short of the levels of protection needed today. The accomplishments below demonstrate NIST's continued dedication to the role it has fulfilled for nearly 50 years – leading public and private collaborations to foster continued improvement and reliability in cryptographic techniques and technology.

Post-Quantum Cryptography

In recent years, there has been steady progress in building quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. When the capacity to build large-scale quantum computers exists, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere. The goal of post-quantum cryptography (PQC) (also called quantum-resistant or quantum-safe cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers and that can be deployed without drastic changes to existing communication protocols and networks.

The question of when a large-scale quantum computer will be built is a complicated one. In the past, it was less clear that large quantum computers were a physical possibility, but many scientists now believe it to be merely a significant engineering challenge. Some engineers even predict that within the next 20 years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use. Historically, it has taken decades to deploy modern public-key cryptography infrastructures, so efforts to prepare information security systems that are resistant to quantum computing must begin now.

Motivated by these considerations, NIST is in the process of selecting public-key (quantum-resistant) cryptographic algorithms through a public, competition-like process. The intent is for new public-key cryptography standards to specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide and capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

In FY 2020, based on public feedback and internal reviews of the candidates, NIST announced the 15 algorithms that would move into the third round of analysis. NIST mathematicians and computer scientists consider these algorithms to be the strongest candidates for standardization. The list includes seven “finalists” for public-key encryption/key-establishment and digital signature algorithms as well as eight “alternates,” which will likely need another round of evaluation. (The complete list is available on the NIST website and is described in NISTIR 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*). At the conclusion of the third round, NIST will select some of the finalists for standardization.

This accomplishment represents several years of intensive research and industry collaboration. NIST appreciates all submitters and those providing comments during the evaluation process. NIST will continue to work with the cryptographic community to analyze the performance of these algorithms to understand how they will perform in the real world.

Lightweight Cryptography

Many elements of modern technology rely on cryptography to provide confidentiality and to ensure the integrity of information being exchanged. While many of today’s cryptographic methods are reliable, they require time and power that many devices (e.g., sensor networks, healthcare products, distributed control systems, IoT, and cyber-physical systems) may not have. The small and simple nature of the millions of electronic devices making up the IoT renders them ill-equipped to process the current cryptographic algorithms. To address this challenge, NIST has initiated a lightweight cryptography standardization process to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable for use in constrained environments where the requirements and performance of the currently approved NIST cryptographic algorithms are not acceptable. In FY 2019, NIST published a call for algorithms to be considered for lightweight cryptographic standards. NIST received 57 submissions, 56 of which were accepted for the first round of evaluation. After four months of evaluation, 32 of the first-round candidates proceeded to the second round of evaluation.

In FY 2020, NIST continued performing a technical review of the second-round candidates. This review included the verification of third-party security analysis; software benchmarking on microcontrollers, determining which candidates perform better than current NIST standards; and investigating the constraints of a variety of use cases.

In November 2019, NIST held the Third Lightweight Cryptography Workshop to discuss the candidate algorithms, including their design strategies, implementations, performance, cryptanalysis, and target applications. In addition, NIST organized a virtual workshop to take place at the start of FY 2021 and continued public collaboration on lightweight cryptography at academic conferences and meetings with industry and government representatives.

Transition to FIPS 140-3

NIST has continued to develop new tools and processes to support an ISO-based cryptographic module testing program as a validation authority while supporting the existing validation process. For more than a quarter of a century, NIST’s FIPS 140 publication series has been used to coordinate requirements and standards of cryptographic modules for use by U.S. agencies.

In March 2019, the Secretary of Commerce approved FIPS 140-3, *Security Requirements for Cryptographic Modules*. The update to FIPS 140 includes references to two existing international standards: ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*; and ISO/IEC 24759:2017, *Information technology — Security techniques — Test requirements for cryptographic modules*.

In support of this update, NIST developed a series of draft Special Publications (the SP 800-140x “subseries”) for public comment. They directly support FIPS 140-3 and its associated program, the Cryptographic Module Validation Program (CMVP):

- Draft SP 800-140, *FIPS 140-3 Derived Test Requirements (DTR)*
- Draft SP 800-140A, *CMVP Documentation Requirements*
- Draft SP 800-140B, *CMVP Security Policy Requirements*
- Draft SP 800-140C, *CMVP Approved Security Functions*
- Draft SP 800-140D, *CMVP Approved Sensitive Parameter Generation and Establishment Methods*
- Draft SP 800-140E, *CMVP Approved Authentication Mechanisms*
- Draft SP 800-140F, *CMVP Approved Non-Invasive Attack Mitigation Test Metrics*

Table 1 describes the transition timeline for implementation of the new standard.

Table 1: Timeline for Implementation of FIPS 140-3 Submissions

Date	Activity
Mar 2019	FIPS 140-3 Approved
Sep 2019	FIPS 140-3 Effective Date
Oct 2019	Drafts of SP 800-140x for public comment
Mar 2020	Published SP 800-140x documents Implementation Guidance updates Tester competency exam updated Updated CMVP Program Management Manual
Sep 2020	CMVP accepts FIPS 140-3 submissions
Sep 2021	CMVP stops accepting FIPS 140-2 submissions for new validation certificates
Sep 2026	Remaining FIPS 140-2 certificates moved to the Historical List

Cryptographic Programs and Laboratory Accreditation

Cryptographic Security Testing laboratories are key to assuring that government systems protected by cryptography to meet the validation requirements. There are currently 20 laboratories around the world certified through the National Voluntary Laboratory Accreditation Program (NVLAP). To better assess tester proficiency knowledge across all laboratories, the Cryptographic Validation Program (CVP) Certification Exam was revamped to update the older FIPS 140-2 exam and incorporate the 2019 FIPS 140-3 standard's unique requirements.

Cryptographic Module Validation Program (CMVP)

If the use of cryptography is needed for the protection of sensitive unclassified information, federal agencies must use validated cryptographic modules. The Cryptographic Module Validation Program (CMVP) was created to support the federal user community's need for strong, independently tested, and commercially available cryptographic modules. In FY 2020, the CMVP awarded 180 new validation certificates. In addition to working with U.S. and Canadian agencies, NIST has begun incorporating standards from international organizations that represent both public and private sectors within the cryptographic community.

In order to remain effective, additional CMVP efforts included:

- Retooling automation to streamline the validation process and improve review consistency;
- Strengthening the relationship with the Cryptographic Module User Forum (CMUF) by collaborating on new and improved technical guidance and programmatic issues; the CMUF FIPS 140-3 working group contributed heavily to the development of training materials and implementation guidance for the new standard;
- Supporting the International Cryptographic Module Conference (ICMC) committee to build relationships with vendors and laboratories and participating in the 2020 ICMC conference;
- Hosting two virtual Lab Manager meetings to keep Cryptographic and Security Testing (CST) laboratories abreast of changes and developments; and
- Developing documents and processes to support the new FIPS 140-3 standard so that the CMVP can accept FIPS 140-3 submissions; the transition to the FIPS 140-3 standard continues as FIPS 140-2 begins to be phased out.

Cryptographic Algorithm Validation Program (CAVP)

The Cryptographic Algorithm Validation Program (CAVP) reached a milestone with the retirement of the Cryptographic Algorithm Validation System (CAVS) test tool. CAVP now performs all algorithm validations using the server-based Automated Cryptographic Validation Test System (ACVTS), which implements the open standard Automated Cryptographic Validation Protocol (ACVP). ACVTS effectively validates algorithm implementations and can make a validation certificate publicly available in minutes. It also enables new testing techniques to be explored and implemented.

At the 2020 RSA Conference, Researchers from NIST's Security Testing, Validation and Management (STVM) group presented a new test capable of detecting a denial-of-service attack for hash functions and digital signature algorithms. STVM researchers have also collaborated with industry researchers to generate high assurance cryptographic tests that have been implemented on the ACVTS server.

8 | Trustworthy Networks



Credit: Shutterstock

NIST works with industry to develop the measurement science and standards necessary to ensure the robustness, scalability, and security of important infrastructures, including mobile telecommunications networks and the global Internet. Research focuses on the measurement and modeling techniques necessary to understand, predict, and control the behavior of Internet-scale networked information systems. NIST staff use these insights to guide the design, analysis, and standardization of new technologies aimed at improving the robustness and reliability of the global communication infrastructure. Much of the research and industry collaboration occurs at NIST's National Cybersecurity Center of Excellence (NCCoE).

NIST's Trustworthy Networks Program works with industry to resolve systemic vulnerabilities in existing and emerging critical network infrastructures and to advance the development of potentially disruptive technologies to improve the trustworthiness of future networks. NIST collaborates directly with leading industry research (Internet Research Task Force), standards (Internet Engineering Task Force), and network operations (North American Network Operators Group) groups to promulgate NIST contributions and foster the design, standardization, and commercial deployment of trustworthy communication infrastructures.

Major research areas and selected recent contributions within this program included:

- The Robust Interdomain Routing Project that works with Internet industry partners to improve the security and resilience of the Internet's global routing infrastructure. NIST SP 800-189, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, includes guidance on securing interdomain routing control traffic, preventing IP address spoofing,

and certain aspects of denial of service (DoS) and distributed DoS (DDoS) detection and mitigation. Many of the recommendations in this publication focus on the Border Gateway Protocol (BGP). Technologies recommended in this document for securing the interdomain routing control traffic include Resource Public Key Infrastructure (RPKI), BGP origin validation, and prefix filtering. Additionally, technologies recommended for mitigating DoS/DDoS attacks focus on preventing IP address spoofing using source address validation with access control lists and unicast reverse-path forwarding. Other technologies – such as remotely triggered black hole filtering, flow specification, and response rate limiting – are also recommended as part of the overall security mechanisms.

- SP 800-189 is referenced in NIST SP 800-53, Revision 5, as the technical basis for new boundary protection security controls (SC-7) that are focused on DDoS mitigation and the prevention of unauthorized control traffic. The guidance also fulfills a significant deliverable described in Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.


Zero Trust Networks

Zero Trust is the term for a set of cybersecurity paradigms to move network defenses from static, physical, network-based perimeters to software-defined security mechanisms based on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan enterprise infrastructure and workflows.

Zero trust assumes that there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., a local corporate network versus the Internet). It is a response to enterprise network trends, including remote users and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources rather than network segments, as the network location is no longer considered the prime component to the security posture of the resource.

NIST SP 800-207, *Zero Trust Architecture*, was published in August 2020 and discusses the core principles and logical components that make up a ZTA. SP 800-207 contains a ZTA definition and describes general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture. Following the publication of SP 800-207, the NCCoE initiated a new ZTA building block demonstration project that is planned to start in FY 2021.

NIST's Software Defined and Virtual Networks Project advances the state of the art in network virtualization, network service function chaining, software-defined networks (SDN), technologies, and techniques to address the robustness and security of virtualized network services. Recent work explores novel applications of network function virtualization (NFV) and SDN to practices such as network security and intrusion detection, cloud computing, machine-to-machine communications, and advanced mobility. A key research component is the development of programmable measurement techniques that efficiently operate at the scale and speed of advanced networks.



The Trustworthy Intelligent Networks project works with industry and academia to improve the trustworthiness and applicability of artificial intelligence and machine learning (AI/ML) technologies in future networks and distributed systems. Research focuses on applications of AI/ML to address security and robustness issues in today's networks and the development of a means to test and measure the robustness of the AI/ML techniques necessary for future autonomic networks.

5G Cybersecurity

The NCCoE announced a 5G Cybersecurity project in the Federal Register in May 2020. The center has invited an impressive roster of technology providers and industry experts to collaborate on its 5G Cybersecurity Project, including AML, AT&T, CableLabs, Cisco, Dell, Intel, Keysight, MiTAC, Nokia, Palo Alto Networks, and T-Mobile. These collaborators will work with the NCCoE 5G team to identify 5G use case scenarios and demonstrate how components of the 5G architecture can provide security capabilities to mitigate identified risks and comply with industry sector requirements. The result will be a publicly available NIST Cybersecurity Practice Guide in the Special Publication 1800 series, describing the practical steps needed to implement a cybersecurity reference design.

Public Safety Communications Research

The Public Safety Communications Research (PSCR) Division serves as a technical advisor and laboratory. PSCR is driven to advance communications technologies for public safety workers by accelerating their development, adoption, and implementation so that the public safety community can more effectively carry out their mission to protect lives and property.

Improving Wearable Device Cybersecurity for Public Safety

In partnership with PSCR, NIST finalized NISTIR 8196, *Security Analysis of First Responder Mobile and Wearable Devices*, which helps consider various threats to and security objectives for new types of products (e.g., smartphones, tablets, wearable devices) that have been made available to public safety via the proliferation of the Nationwide Public Safety Broadband Network (NPSBN). Its goals are to help public safety organizations make informed decisions when selecting wearable technology and to better inform industry about cybersecurity concerns of the public safety use case.

Innovations in Novel Technologies

NIST researchers designed and implemented a PSCR Prize Challenge – Making the Case: Proactive Image Protection, one of ten challenges within the Tech to Protect Challenge. The contest tasked participants with designing a system that could identify the provenance and prove the authenticity of an image captured on a mobile device being used for public safety purposes. NIST awarded prizes to four finalists whose solutions stand to build more confidence in digital images gathered by public safety and law enforcement.

Advancing Authentication Technology for Public Safety

The embrace of Long Term Evolution (LTE) mobile communications technology has led to critical cybersecurity challenges for public safety, including authentication and identity management. The mechanisms used in consumer devices do not sufficiently meet the public's safety needs.

To stimulate innovation in authentication technology, researchers implemented an Open Innovation Challenge: Expanding SIM Card Use for Public Safety. With the introduction of the Nation's first public safety-focused LTE network, this challenge asked the question, "Can public safety leverage the universal integrated circuit card (UICC), a technology that is already integrated into the LTE technology stack, to implement multi-factor authentication?" NIST awarded cash prizes to three finalists who each demonstrated proof-of-concept solutions to this question.

PSCR, in partnership with NCCoE, identified critical technology areas that will likely influence the public safety technology field in the near future. Over the past year, the team has worked to produce several informative and guiding resources for stakeholders that describe technology impacts, considerations, and best practices. These publications will lay a common groundwork for the field before individual public safety agencies begin to implement security solutions in identity federation, Identity as a Service (IDaaS), and biometric authentication. The PSCR/NCCoE partnership has also awarded a grant to the Georgia Tech Research Institute (GTRI) to further support their Trustmarks project, which seeks to build a system to support identity federation and information sharing by establishing requirements and capabilities for identity providers.

9 | Trustworthy Platforms



Credit: Shutterstock

NIST defines a platform as a computer or hardware device or associated operating system, or a virtual environment, on which software can be installed or run. The goal of the Trustworthy Platforms focus area is to improve trust in the security and privacy of these systems and infrastructures by providing guidance and technologies for the development and use of secure platforms, including software, hardware, and firmware. The trustworthy platform is a dynamic ecosystem that depends on multiple security and privacy technologies in order to reliably deliver its services to the users. It is deployed and maintained in a measured state that is known to protect the security and privacy of users and data, and it performs services in a consistent and reliable manner. The desired outcome is to increase the adoption of trustworthy platforms in order to improve trust in the security and privacy of systems and infrastructures. NIST provides guidance and technologies for the development and use of secure platforms and foundational components such as cryptography. NIST also helps to develop quantifiable measurements that provide assurances for platform security, privacy, and robustness.

Secure Software Development Framework

The software development life cycle (SDLC) is a methodology for designing, creating, and maintaining software. Though there are many SDLC models, most do not explicitly address software security.

Secure software development practices should be integrated throughout SDLC models for three reasons:

1. To reduce the number of vulnerabilities in released software,
2. To mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and
3. To address the root causes of vulnerabilities to prevent future recurrences.

In April 2020, NIST published the final version of a Cybersecurity White Paper on secure software development practices, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*. The white paper recommends a core set of high-level secure software development practices – called the Secure Software Development Framework (SSDF) – to be added to each SDLC implementation. The SSDF practices are based on those from established secure software development practice documents by other organizations. The SSDF also provides a common vocabulary for secure software development that software consumers can use to foster communications with software suppliers in acquisition processes and other management activities.

Since NIST published the SSDF, there has been considerable interest from industry and others in NIST in illustrating how the SSDF can be applied to particular SDLC models, especially transitioning DevOps implementations to DevSecOps. NIST will continue to refresh and evolve the SSDF in response to public feedback and the changing threats, vulnerabilities, practices, and automation capabilities in software development.

Industrial Control System (ICS) Cybersecurity and Manufacturing Profile

A revision to NISTIR 8183, *Cybersecurity Framework Manufacturing Profile*, includes the subcategory enhancements established in the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. These updates also include managing cybersecurity within the supply chain, self-assessing cybersecurity risk, vulnerability disclosure, system integrity, and more comprehensive controls for identity management.

The Manufacturing Profile was developed for manufacturers managing cybersecurity risk and is aligned with manufacturing sector goals and industry best practices. It provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Systems Security Engineering

In FY 2020, NIST continued to foster the engineering-driven perspectives and actions necessary to develop more defensible and survivable systems, including the machine, physical, and human components of systems and the capabilities and services delivered by those systems. The Systems Security Engineering (SSE) approach builds upon well-established international standards for systems and software and fuses systems security engineering methods, practices, and techniques. The initial volume in this new series, SP 800-160, Volume 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, describes an approach to designing, building, and retrofitting engineered systems with the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems

that use or are enabled by cyber resources. Volume 2 provides a handbook for achieving the identified cyber resiliency outcomes based on a systems engineering perspective on system life cycle and risk management processes. Organizations can select, adapt, and use some or all of the cyber resiliency constructs and apply the constructs to the technical, operational, and threat environments for which systems need to be engineered.

Smart Grid Cybersecurity

In FY 2020, engineers from NIST's Engineering Laboratory and ITL expanded on the Cybersecurity Framework Smart Grid Profile created during FY 2019 by developing a draft profile for the specific capability of voltage regulation on the electric distribution system. The draft profile compares and contrasts distribution system voltage regulation for both a high distributed energy resource (DER) environment and a conventional grid environment and prioritizes NIST Cybersecurity Framework subcategory outcomes based upon their ability to assist power system stakeholders in achieving voltage regulation within these environments.

Working with a representative from the North American Electric Reliability Corporation (NERC), NIST helped update the mapping between the NERC Critical Infrastructure Protection (CIP) requirements and version 1.1 of the NIST Cybersecurity Framework. They also collaborated with industry volunteers to help create a self-assessment tool for utilities to measure their cybersecurity and compliance maturity and develop an improvement plan. NIST continues to chair the Smart Electric Power Alliance (SEPA) cybersecurity working group and has established an effort to determine threats to the power grid posed by customer energy Internet of Things (IoT) devices (e.g., smart thermostats and water heaters) and provide suggested mitigations.

Methods for Securing Virtual Infrastructure

Microservices—an approach to software development using independent but interconnected applications—simplify software scalability, usability, and availability. Because of these benefits, this type of architecture is becoming commonplace for cloud-based and large enterprise applications, but the characteristics of microservices-based applications bring increased security challenges. The sheer number of microservices results in more interconnections and more communication links to be protected. Additionally, the ephemeral nature of microservices calls for secure service discovery mechanisms and the deployment of security services that are not tightly coupled with application code. Given the characteristics and associated security challenges, point security solutions (e.g., authentication, authorization, security monitoring) are inadequate.

In FY 2020, NIST published SP 800-204A, *Building Secure Microservices-based Applications Using Service Mesh Architecture*. The publication provides deployment guidance for proxy-based service mesh components as well as secure configuration recommendations that span the entire application infrastructure space.

ITL Leadership and Participation in National and International Standards Programs

During FY 2020, NIST staff contributed to and held leadership positions in various standards developing organizations (SDOs), including the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), and the ISO/IEC. Staff actively participated in standards bodies to raise awareness and influence the development of privacy and cybersecurity standards, including efforts within the ISO/IEC.

In FY 2020, NIST continued to engage with government and industry organizations to demonstrate and ensure continued alignment with voluntary international standards. NIST discussed the Cybersecurity Framework in numerous dialogues and has continued to identify and promote international adaptations and translations of the Framework. NIST also continues to contribute to international standards development efforts related to cybersecurity risk management and the development of cybersecurity frameworks, including ISO/IEC Technical Specification 27110.

The standards community is built upon international collaboration, and NIST leverages its foundational and applied research efforts and experience in leadership to contribute to the development of national and international standards. Today, these standards activities span cybersecurity, privacy, cryptography, and critical fields, such as 5G mobile and cellular technologies, quantum information, cloud, blockchain and distributed ledger technologies, and the Internet of Things (IoT).

About 70 NIST staff members work with other agencies and industry leaders to develop cybersecurity and privacy standards through voluntary consensus. NIST's standards strategy is captured in NISTIR 8074, *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives or Cybersecurity*.

NIST has been instrumental in promoting and participating in the development of a family of voluntary ISO/IEC standards that align with NIST's cryptographic module validation standard and related specifications. NIST served as the project editor for nine of those standards. NIST uses collaborative opportunities to highlight the role that standards play in enabling technological innovation and interoperability among products and systems. International collaboration and alignment on standards-based approaches to cybersecurity and privacy risk management lead to greater innovation and a more effective and efficient utilization of resources.

NIST also shares information on standards processes, the importance of standards on the economy and facilitating international trade, and the ability of standards to help secure systems and infrastructure. NIST coordinates with interagency partners on strategic approaches and communication on standards for the U.S. Government.

In FY 2021, NIST staff will continue to lead and participate in cybersecurity and privacy standardization efforts with an increased focus on new and emerging areas, such as AI, quantum information, 5G communications, and zero trust architectures.

Opportunities to Engage with the NIST Cybersecurity & Privacy Program

Stakeholders are an important force behind NIST's cybersecurity and privacy programs. NIST counts on developers, providers, and everyday users of cybersecurity and privacy technologies and information to guide priorities in serving the public and private sectors. Stakeholders are also vital when it comes to decisions about the best methods and formats for delivering information and services.

NIST engages in many ways, both formal and informal. NIST participates in various forums, Communities of Interest (COI), joint research efforts, standards development organizations, Guest researcher projects, student programs, and other partnership opportunities that are available; hosts/sponsors various cybersecurity and privacy events; and gathers public feedback on NIST publications, blogs, and social media.

Further details on engaging with NIST on Cybersecurity and Privacy are available at <https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement>.

Funding Opportunities at NIST

NIST funds industrial and academic research in several ways. The Small Business Innovation Research Program funds research and development (R&D) proposals from small businesses. NIST offers grants to encourage work in the fields of precision measurement, fire research, and materials science. Grants and awards supporting research by industry, academia, and other institutions are also available on a competitive basis through various Institute offices.

For general information on the NIST grants programs, please contact Mr. Christopher Hunton at (301) 975-5718 or by email at grants@nist.gov.

STAY IN TOUCH

CONTACT US

 [NIST.gov/cybersecurity](https://www.nist.gov/cybersecurity)  Cybersecurity-Privacy@NIST.gov  [@NISTcyber](https://twitter.com/NISTcyber)

AUTHORITY

This publication has been developed by the National Institute of Standards and Technology (NIST) in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA of 2014, 44 U.S.C. § 3541. 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 be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-214
Natl. Inst. Stand. Technol. Spec. Publ. 800-214, 37 pages (September 2021)

CODEN: NSPUE2

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.800-214>

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 who provided write-ups on their project highlights and accomplishments for this annual report. They appreciate the work of Elaine Barker, Lisa Carnahan, Neal Gammons, Sara Kerman, Jeff Marron, Sheryl Taylor, and Isabel Van Wyk for reviewing and providing valuable feedback for this annual report.

TRADEMARK INFORMATION

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

BACKGROUND INFORMATION OF ANNUAL REPORT

This Annual Report provides the opportunity to describe the many cybersecurity program highlights and accomplishments from throughout the NIST Information Technology Laboratory (ITL). The report is organized into several focus areas that highlight key research topics and highlights.

Please note: This Annual Report covers the Federal Government's Fiscal Year (FY) 2020, from October 1, 2019 to September 30, 2020.

ITL, an operating unit under NIST, contains seven divisions. Cybersecurity work is conducted by each division, and it is the sole focus of the Applied Cybersecurity and Computer Security Divisions. Throughout this Annual Report, there are references to particular division activities and often to work by groups within those divisions.

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (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.

