2020 Cybersecurity and Privacy Annual Report

National Institute of Standards and Technology
U.S. Department of Commerce

NIST SPECIAL PUBLICATION 800-214

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

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 Proo ing*; 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

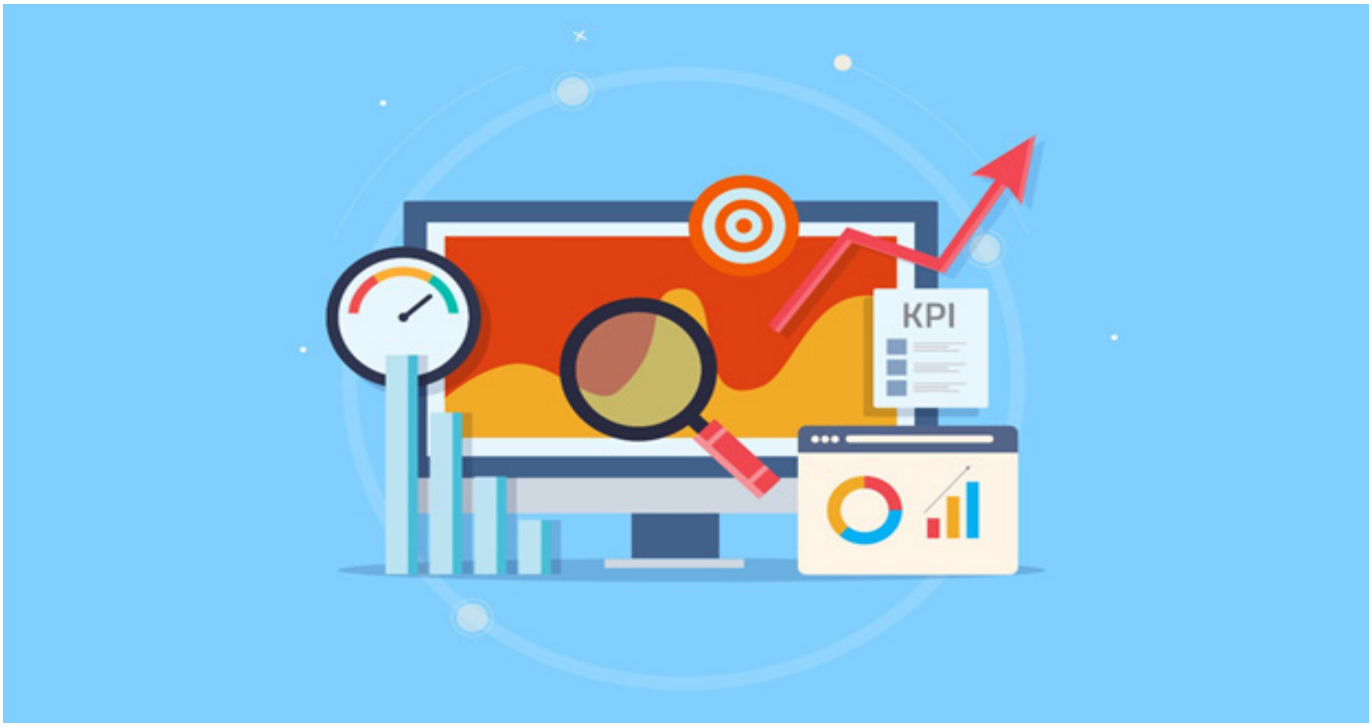
NIST developed SP 800-210, General Access Control Guide for Cloud Systems, to present cloud access control characteristics and general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). The main focus is 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.