NIST SPECIAL PUBLICATION 800-211

2019 ANNUAL REPORT

NIST/ITL CYBERSECURITY PROGRAM

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

THIS PAGE IS INTENTIONALLY LEFT BLANK

Front cover image credit: Shutterstock / Khakimullin Aleksandr

NIST SPECIAL PUBLICATION 800-211

ANNUAL REPORT 2019

NIST/ITL CYBERSECURITY PROGRAM

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.800-211

AUGUST 2020

U.S. DEPARTMENT OF COMMERCE
Wilbur L. Ross, Jr., Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

AUTHORITY

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

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

National Institute of Standards and Technology Special Publication 800-211
Natl. Inst. Stand. Technol. Spec. Publ. 800-211, 60 pages (August 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-211

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: cybersecurity.annualreport@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) 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 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.

ABSTRACT

During Fiscal Year 2019 (FY 2019), from October 1, 2018 through September 30, 2019, the NIST Information Technology Laboratory (ITL) Cybersecurity and Privacy Program successfully responded to numerous challenges and opportunities in security and privacy. This annual report highlights the FY 2019 research agenda and activities for the ITL Cybersecurity and Privacy Program, including: the ongoing participation and development of international standards; the enhancement of privacy and security risk management models, including those for the protection of controlled unclassified information (CUI), systems engineering and cyber resiliency, supply chains, and mobile technologies; the continued advancement of cryptographic technologies, including updates to Federal Information Processing Standard (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*, and preparation for post-quantum cryptographic methods; and improved infrastructure protection in areas such as zero trust architectures and advanced networking security. NIST maintained a strong focus on supporting small and medium-sized businesses (SMBs), including updates to the Small Business Cybersecurity Corner website to make resources easier to find and use, and drawing on contributed cybersecurity resources and feedback received from federal partners and the public.

KEYWORDS

annual report; Advanced Network Technologies Division; ANTD; Applied Cybersecurity Division; ACD; Computer Security Division; CSD; Cybersecurity; Cybersecurity Program; Federal Information Security Management Act; FISMA; privacy; program highlights; Information Access Division; IAD; information security; Information Technology Laboratory; ITL; program accomplishments; Software and Systems Division; SSD.

TABLE OF CONTENTS

THIS PAGE IS INTENTIONALLY LEFT BLANK

FOREWORD

Last year's annual report on cybersecurity noted that NIST is "picking up the pace" in advancing cybersecurity and privacy, and a look back at Fiscal Year 2019 proved that to be an understatement. The year witnessed a significant increase in the degree and kind of our collaborations to expand and improve the building blocks of cybersecurity.

That greater collaboration helped us deal with the ever-quickening speed of technological changes that present one challenge after another in cybersecurity. By working closely with partners in the private sector, universities, and other agencies both in the United States and abroad, NIST made great progress in researching and providing practical methods to achieve improved security and privacy risk management, stronger cryptography, more secure communications, more reliable automation, and to better understand, advance, and utilize other foundational elements of cybersecurity.

Helping organizations to better manage security and privacy risk, we updated the *Risk Management Framework* to even more fully support organizational security and privacy at all levels. Through a series of workshops and online forums, we brought industry and government together to create the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. The NIST *Cybersecurity Framework* continues to gain users as companies and government organizations around the world have recognized the value of that model and are translating it, tailoring it to adapt to local needs, and using it to provide a common language for communicating about and achieving good cybersecurity risk management practices.

The world of cryptography is getting larger and smaller at the same time. This report describes some of the notable accomplishments in NIST's continuing quest with our collaborators to evaluate and standardize quantum-resistant public-key cryptographic algorithms. At the other end of the spectrum, we advanced lightweight cryptography to balance the security needs for circuits smaller than were even dreamed of just a few years ago.

NIST's work on secure software development and systems engineering reinforces the need to design and implement software and systems that are secure, resilient, and trustworthy from the start—a theme that runs throughout many of the resources we produced and updated in FY 2019 and describe in this report.

Advances in new and emerging technologies and approaches like blockchain, artificial intelligence, 5th Generation (5G) communications, secure infrastructure, zero trust architecture, and the Internet of Things are enabling new and remarkable products. The accomplishments and activities in this report demonstrate how NIST continues to work with industry partners to ensure that evolving technologies are secure, reliable, and trustworthy—now and into the future.

The year marked a decade of progress by the NIST-managed National Initiative for Cybersecurity Education (NICE), to help the world address the human element of cybersecurity from the classroom to the workplace. Tackling the shortage of cybersecurity talent has become an even more urgent priority for NIST and its collaborators, with FY 2019 being an especially productive year.

We kept our promise to pick up the pace, and we are excited to see what Fiscal Year 2020 has in store. We invite you to learn more about these programs and to join us as we continue to build a better future on these foundations!

Donna Dodson
NIST Chief Cybersecurity Advisor

CREDIT: iStock / ipopba

FOCUS AREA 1: ADVANCING CYBERSECURITY AND PRIVACY STANDARDS

Leadership and Participation In Developing National and International Standards

The standards community is built upon international collaboration. NIST leverages its foundational and applied research efforts along with its 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, and the Internet of Things (IoT).

About 40 NIST staff members work with other agencies and industry to develop cybersecurity and privacy standards through voluntary consensus Standards Developing Organizations (SDOs). NIST's standards strategy is captured in NIST Interagency Report (NISTIR) 8074, *Cybersecurity Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*.

During FY 2019, NIST staff actively contributed to and held leadership positions in various SDOs, including the International Electrotechnical Commission (IEC), the Internet Engineering Task Force (IETF), and the International Organization for Standardization (ISO). The NIST staff actively participated in standards bodies to raise awareness and influence the development of privacy and cybersecurity standards, including efforts within the ISO/IEC joint technical committee (JTC) 1 Subcommittee (SC) 27, that aligned with the principles of the NIST Cybersecurity Framework. NIST representatives also

participated in the ISO Project Committee (PC) 317, which focuses on developing ISO 31700, *Consumer protection: privacy by design for consumer goods and services*. The NIST staff worked to promote the development and international use of the NIST Privacy Framework and its principles through engagement with several privacy standards activities from the Institute for Testing and Certification (ITC).

NIST participation has also grown considerably in IoT standardization activities, including:

- ISO JTC 1/SC 41, *IoT architecture and vocabulary, IoT Interoperability, and IoT Applications*;
- ISO JTC 1/SC 27, *IoT aspects of Security and Privacy*; and
- IETF, *Software Updates for Internet of Things* Security Area.

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 serves as the project editor for nine of those standards. Federal Information Processing Standard (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*, points to ISO/IEC 19790, *Security Requirements for Cryptographic Modules*. [1] Testing for these requirements will be performed in accordance with ISO/IEC 24759, *Test Requirements for Cryptographic Modules*. This is an ongoing effort and will continue over the next several years to support a smooth transition path to those using FIPS 140-3 specifications.

In FY 2020, the 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 artificial intelligence (AI), quantum information, and IoT. NIST will continue to provide thoughtful leadership in many SDOs by actively participating in those organizations and contributing publications and papers.

CREDIT: Shutterstock / bleakstar

FOCUS AREA 2: ENHANCING RISK MANAGEMENT

NIST has made significant progress during FY 2019 in advancing methods and guidelines for managing organizational risk related to cybersecurity, systems engineering, and privacy. While risk management has been a fundamental driver for organizations for as long as there has been information to protect, advances in technology increasingly call for a collaborative approach to engineering secure systems, securing systems managed by external partners, and applying risk management to an ever-evolving range of products.

Notable achievements during FY 2019 included updates to several NIST endeavors that are described below.

The Next-Generation Risk Management Framework

The Risk Management Framework (RMF) is one of NIST's most highly 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. The RMF includes processes for information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. It also includes activities to prepare organizations to execute the RMF at appropriate risk management levels.

In FY 2019, NIST published SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [2]. SP 800-37, Rev. 2, represents the next-generation Risk Management Framework (RMF) for systems, organizations, and individuals. The updates include an

initial alignment with the constructs in the NIST Cybersecurity Framework, the integration of privacy risk management processes, an alignment with system life-cycle security engineering processes, and the incorporation of supply chain risk management processes.

This is the first NIST publication to include a full integration of privacy risk management into the existing information security risk management processes. The addition of a new **Prepare** step is one of the key changes to the RMF and was incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. The new step works in harmony with the *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the *NIST Cybersecurity Framework*) and the NIST *Privacy Framework* [3] [4]. The use of these models together institutionalizes organization-level and system-level preparation by:

- Facilitating communication across the organizational risk management levels;
- Encouraging the organization-wide identification of common controls and the development of organizationally tailored control baselines;
- Reducing the complexity of the IT infrastructure; and
- Providing additional methods to identify, prioritize, and focus resources on high-value assets commensurate with risk.

NIST has also continued to support public and private-sector outreach and products for the risk management community. For example, NIST hosted a well-attended webcast about the RMF updates and developed an online reference site for multiple electronic formats of the security and privacy controls from NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* [5].

Advancement of Privacy Engineering and Risk Management

NIST made significant advances in guidance and models for managing privacy risks in FY 2019. These privacy risks can have direct adverse consequences at both the individual and societal levels, with follow-on effects on organizations' brands, bottom lines, and future growth prospects. NIST is dedicated to supporting innovation that provides the benefits of information processing while simultaneously applying methods that help protect the privacy of individuals.

While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient. Cybersecurity and privacy have both unique and overlapping risk management needs, as illustrated by Figure 1: Cybersecurity and Privacy Risk. Having a general understanding of the different origins of cybersecurity and privacy risks is important for determining the most effective solutions to address the risks.

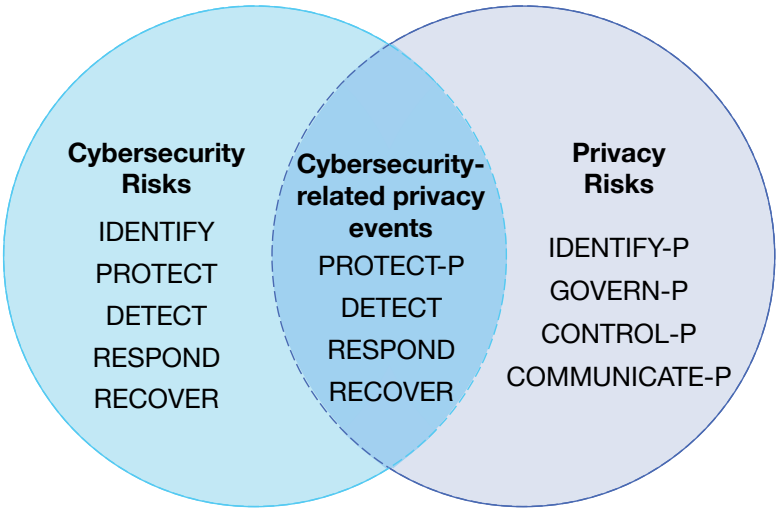


Figure 1: Cybersecurity and Privacy Risk

FY 2019 was a busy and fruitful year of open collaboration with stakeholders from across government, academia, and industry who worked together to craft and hone tools, standards, and processes to better identify, prioritize, and manage privacy risks. NIST also collaborated on the creation of the NIST *Privacy Framework: An Enterprise Risk Management Tool* [4], which addresses the need to manage privacy issues across the U.S. and throughout the world, improve privacy protections, and better manage compliance with increasing global privacy requirements. The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and organizations, and stay current with technology trends such as AI and IoT. The Privacy Framework follows the structure of the NIST Cybersecurity Framework, facilitating the use of both frameworks together. Each framework component reinforces privacy risk management through the connection between business and mission drivers, organizational roles and responsibilities, and privacy protection activities. The Privacy Framework was developed from comments to public requests for information (RFI) and discussions during three public workshops, five webinars, and hundreds of direct interactions with stakeholders. A public draft was released at the end of FY 2019, and the subsequent final version was released in early FY 2020.

While the Privacy Framework represents a great leap forward in the privacy risk management space, NIST also supported advancement in several areas of privacy engineering in FY 2019.

- NIST guidance has sought to highlight the importance of security and privacy for all organizations and enterprises. Privacy aspects were subsequently integrated into many of NIST's publications, such as SP 800-37, Revision 2, and NISTIR 8228, *Considerations for Managing IoT Cybersecurity and Privacy Risks* [6].

- NIST has driven change and standardization through leadership positions in many key organizations. The NIST staff fills leadership positions in key organizations, including membership in the Privacy Engineering Advisory Board for the International Association of Privacy Professionals (IAPP), co-chairmanship of the Interagency Working Group (IWG) for Privacy at the U.S. Networking and Information Technology Research and Development (NITRD), and working group chairmanship at ISO Technical Committee ISO/PC 317, *Consumer protection: privacy by design for consumer goods and services*. Through these and many other programs, NIST provides leadership and direction and helps drive application standards for important risk management focus areas.
- NIST has fostered leadership and partnership through the Privacy Collaboration Space—an online venue open to the public where practitioners can discover, share, discuss, and improve upon open-source tools, solutions, and processes that support privacy engineering and risk management. Following the NIST tradition of open and transparent partnerships, the collaboration space was launched with an initial focus on:
    - De-identification: a technique or process applied to a dataset with the goal of preventing or limiting certain types of privacy risks to individuals, protected groups, and establishments while still allowing for the production of aggregate statistics. This focus area includes a broad scope of de-identification to allow for noise-introducing techniques, such as differential privacy, data masking, and the creation of synthetic datasets that are based on privacy-preserving models.
    - Privacy Risk Assessment: a process that helps organizations to analyze and assess privacy risks for individuals that arise from the processing of their data. This focus area includes risk models, risk assessment methodologies, and approaches to determining privacy risk factors. Through the new space, which is enabled by the Github repository, the community can contribute to privacy engineering in the form of tools, use cases, and feedback on existing entries.

Advancing the Application of the NIST Cybersecurity Framework

Having published the updated Cybersecurity Framework Version 1.1 in FY 2018, NIST continued to work with the risk management community to support outreach, application, and implementation. The NIST Cybersecurity Framework website has expanded to provide learning materials, success stories, and industry resources. Among those resources is NISTIR 8183, *Cybersecurity Framework Manufacturing Profile* [7]. Co-developed with NIST's Engineering Laboratory (EL), this report applies the Cybersecurity Framework components to help describe specific cybersecurity activities and outcomes for the protection of the manufacturing system and its components, facility, and environment.

Another advancement in the application of the Cybersecurity Framework is the implementation of an online catalog of informative references. In FY 2019, NIST launched

the National Cybersecurity Online Informative References (OLIR) Program to facilitate subject matter experts in defining online informative references (OLIRs) between the cybersecurity elements of their documents and the cybersecurity elements of other documents, like the Cybersecurity Framework. The OLIR Program provides a standardized format for expressing OLIRs and a centralized location for accessing and comparing them. NISTIR 8278, *National Cybersecurity OLIR Program: Guidelines for OLIR Users and Developers*, describes the OLIR Program, explains what OLIRs are, how they can be beneficial, and how subject matter experts can contribute OLIRs [8].

The Informative Reference catalog implements a federated model, where submitting parties develop and host their respective Informative References. NIST released NISTIR 8204, *Cybersecurity Framework OLIR Submissions: Specification for Completing the OLIR Template,* which provides guidance to Informative Reference developers for completing and submitting OLIRs [9]. NIST analyzes the submitted OLIRs for correctness, works with submitters regarding any corrections, and hosts links to the public draft and final versions of the OLIRs.

The OLIR Program integrates ongoing NIST projects that respond to administrative and legislative requirements. The OLIR Program can incorporate any authoritative documents, from national and international standards, guidelines, frameworks, and regulations to policies for individual organizations, sectors, or jurisdictions. By following this approach, cybersecurity document owners can use the OLIR Program as a mechanism for communicating with owners and users of other cybersecurity documents.

Protecting Controlled Unclassified Information (CUI)

Other risk management-focused NIST cybersecurity accomplishments in FY 2019 included continued outreach and updates regarding recommendations for protecting the confidentiality of controlled, unclassified information (CUI) in nonfederal systems and organizations. A significant amount of federal CUI is entrusted to external entities. Safeguarding that CUI is of paramount importance and can directly affect the ability of federal agencies to successfully protect their information.

In FY 2019, NIST partnered with the National Archives and Records Administration (NARA)—designated as the CUI Executive Agent by Executive Order 13556, *Controlled Unclassified Information*—on several publications:

- Draft SP 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, provides updates to Chapter One (Introduction), Chapter Two (The Fundamentals), Glossary, Acronyms, and References appendices [10].
- Draft SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*, which provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in SP 800-171, Revision 1 [11].

- Draft SP 800-171B, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets*, which provides enhanced security requirements that apply only to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components when the designated CUI is contained in a critical program or high-value asset [12]. The enhanced security requirements are only applicable to a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement.

In October 2018, NIST coordinated with the Department of Defense (DoD) and NARA to host an informational workshop that provided an overview of CUI, updates about recent changes to CUI provisions in the Defense Federal Acquisition Regulations Supplement (DFARS), and NIST Special Publications 800-171 and 800-171A. This workshop featured panels of Federal Government representatives (who discussed expectations for evaluating evidence and implementing the CUI security requirements) and industry representatives (who shared best practices and lessons learned).

Systems Security Engineering (SP 800-160, Volumes 1 & 2)

In FY 2019, NIST continued to foster the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, including the machine, physical, and human components that compose the 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 objective is to address security issues from the perspective of stakeholder protection needs, concerns, and requirements using established engineering processes so that appropriate fidelity and rigor are addressed early on and in a sustainable manner throughout the life cycle of the system. NIST also published the first draft in a series of specialty publications that were developed to support the NIST SSE guideline. Volume 2 addresses cyber resiliency considerations for two important, yet distinct, communities of interest: 1) those conducting the new development of IT component products, systems, and services and 2) those with legacy systems (having an installed base) currently carrying out day-to-day mission and business functions.

An element of this focus on risk-based SSE included the publication of a new NIST Cybersecurity White Paper entitled, *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* [13]. This white paper builds on a proven software development life cycle (SDLC) methodology for designing, creating, and maintaining software and encouraging the integration of specific secure software development practices. Benefits of SSDF include reducing the number of vulnerabilities in released software, mitigating the potential exploitation of undetected or unaddressed vulnerabilities, and addressing the root causes of vulnerabilities to prevent future recurrences.

The white paper represents an example of the SSE project described above, fostering a subset of high-level practices that are based on established standards, guidance, and secure software development practice documents. These practices, collectively called a secure software development framework (SSDF), should be particularly helpful for the target audiences to achieve security software development objectives. Such a framework is advantageous because an organization in any sector or community, regardless of size or cybersecurity sophistication, can integrate the framework into any existing software development workflow and automated toolchain. It can be applied to typical IT infrastructures as well as more unique models, such as industrial control systems (ICS), cyber-physical systems (CPS), or IoT.

Cyber Supply Chain Risk Management (C-SCRM)

Information and operational technology (IT/OT) rely on a complex, globally distributed and interconnected supply chain ecosystem to provide highly refined, cost-effective, and reusable solutions. This ecosystem is composed of various entities with multiple tiers of outsourcing, diverse distribution routes, assorted technologies, laws, policies, procedures, and practices—all of which interact to design, manufacture, distribute, deploy, use, maintain, and manage IT/OT products and services.

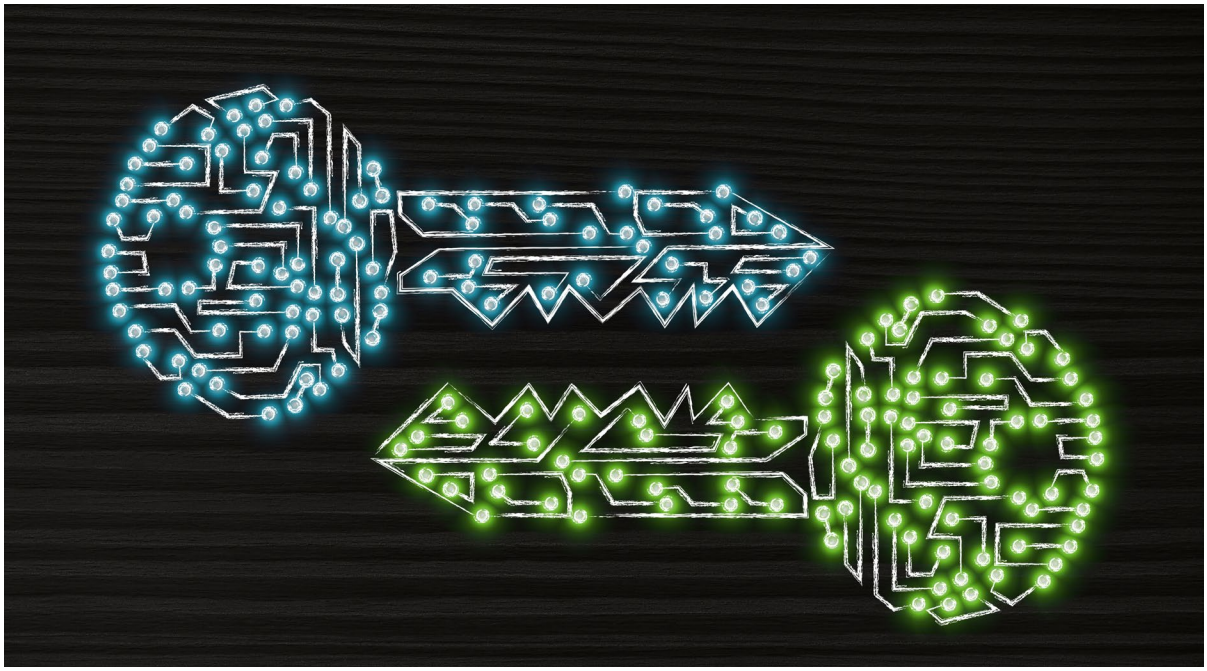
Organizations are increasingly at risk of supply chain compromise, whether intentional or unintentional. Many beneficial factors (e.g., low-cost, interoperability, rapid innovation, and product variety) also increase the risk of a compromise to the cyber supply chain, which may result in risks to the end user. Managing cyber supply chain risks requires ensuring the integrity, security, quality, and resilience of the supply chain and its products and services. Cyber supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, and the insertion of malicious software and hardware as well as poor manufacturing and development practices in the cyber supply chain.

An important NIST initiative is Cyber Supply Chain Risk Management (C-SCRM), the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. C-SCRM is integrated into Systems Security Engineering (described above) and covers the entire system life cycle (including design, development, distribution, deployment, acquisition, maintenance, and destruction) since supply chain threats and vulnerabilities may (intentionally or unintentionally) compromise an IT/OT product or service at any stage.

SCRM work in FY 2019 included:

- Development of the draft NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks*, which 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 [14]. This tool does not represent a complete supply chain risk management solution, but it is intended to be integrated into or used in concert with tools such as third-party management, enterprise resource planning, and supply chain management efforts.

- Participation in the Federal Acquisition Security Council (created as a requirement of the U.S. Federal Acquisition Supply Chain Security Act of 2018). The council helps to develop policies and processes for agencies to use when purchasing technology products. It works closely with many federal entitities (such as the Department of Homeland Security's National Risk Management Center) to support supply chain-related risks in acquisition of items such as: IT, including cloud computing services of all types; telecommunications equipment or telecommunications services; information processing; and IT hardware, systems, devices, software, or services that include embedded or incidental information technology.
- Development of a draft NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, to provide a high-level summary of practices deemed by subject matter experts to be foundational to an effective cyber supply chain risk management program [15]. This work builds on the *Roadmap for Improving Critical Infrastructure Cybersecurity*, a companion document to the NIST Cybersecurity Framework. Since NIST has researched industry practices in cyber supply chain risk management (C-SCRM) through engagement with industry leaders, the group was able to identify some helpful practices. 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.



CREDIT: Shutterstock / faithie

FOCUS AREA 3: STRENGTHENING CRYPTOGRAPHIC STANDARDS AND VALIDATION

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 today would fall far short of the necessary levels of protection. 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 (PQC)

In recent years, there has been a substantial amount of research on quantum computers—machines that exploit quantum mechanical phenomena to solve mathematical 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 (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both

quantum and classical computers and can interoperate with existing communications 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 or so 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 infrastructure, so efforts to prepare information security systems that are resistant to quantum computing must begin now.

NIST is in the process of soliciting, evaluating, and standardizing the needed quantum-resistant public-key cryptographic algorithms. 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 2019, NIST announced the result of its work to winnow the group of potential algorithms to 26. NIST mathematicians and computer scientists consider these algorithms to be the strongest candidates submitted to the Post-Quantum Cryptography Standardization project. The list includes 17 second-round candidates for public-key encryption and key-establishment algorithms as well as nine second-round candidates for digital signatures. (The complete list is available at https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates and is described in NISTIR 8240, *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process* [16].) This accomplishment represents several years of intensive research and industry collaboration. For the next year, NIST will work with the cryptographic community to focus on analyzing the performance of these algorithms to understand how they will perform in the real world.

For several years, NIST has solicited public comments on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The comments received are posted along with a summary of the changes made as a result of these comments. In FY 2019, submissions and comments continued and were shared with the cryptographic community. Additionally, NIST has participated in outreach events such as 2019 Second PQC Standardization Conference at the University of California, Santa Barbara.

NIST extends its appreciation to all submitters and those providing public comments during the post-quantum algorithm evaluation process.

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, distributed control systems, IoT, and cyber-physical systems) may not have available. The small and simple nature of the millions of electronic devices making up the IoT renders them unequipped to process the current cryptographic algorithms. To address this challenge, NIST is working with the cryptographic community to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable for use in constrained environments where the requirements and performance of the current NIST cryptographic standards is not acceptable. NIST published a call for algorithms to be considered for lightweight cryptographic standards in FY 2019.

In FY 2019, NIST also announced the publication of NISTIR 8268, *Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process* [17]. This report described the application of a public, competition-like process to select one or more authenticated encryption and hashing schemes that are suitable for constrained environments. NIST received 57 candidate algorithms for consideration, of which 56 were accepted as first-round candidates. NISTIR 8268 describes the evaluation criteria and selection process based on public feedback and an internal review of the candidates and provides the list of 32 candidate algorithms selected for the second round of the evaluation process. (See https://csrc.nist.gov/projects/lightweight-cryptography/round-2-candidates.) NIST continued public collaboration on the topic in its third gathering at the Lightweight Cryptography Workshop in Gaithersburg, MD, where the candidate algorithms, including their design strategies, implementations, performance, cryptanalysis, and target applications.

Transition to FIPS 140-3

In FY 2019, NIST 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 century, NIST's Federal Information Processing Standard (FIPS) 140 publication series has been used to coordinate the requirements and standards of cryptographic modules for use by U.S. agencies.

CREDIT: Shutterstock / Victor Moussa

On March 22, 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 NIST 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*

NIST has determined a transition timeline for the implementation of the new standard, as described in Table 1: Timeline for Implementation of FIPS 140-3 Submissions.

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	Publication of 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

CREDIT: Shutterstock / Virrage Images

FOCUS AREA 4: ADVANCED CYBERSECURITY RESEARCH & APPLICATIONS DEVELOPMENT

NIST's cybersecurity research and applications development activities include identifying emerging and high-priority technologies, developing security solutions that will have a high impact on the U.S. critical information infrastructure, and developing and showing how to manage foundational building-block security mechanisms and techniques that can be integrated into an organization's mission-critical information systems.

Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data

Virtualization drives much of today's computing, and a basic component of that is the use of hypervisors—the software, firmware, or hardware that creates and runs many virtual machines. Because of the role that hypervisors play in critical technology such as cloud computing, they are often the target of attacks. To help address this need, NIST has developed a methodology to enable forensic analysis on attacks on hypervisors. Two open-source hypervisors—Xen and Kernel-based Virtual Machine (KVM)—were chosen as platforms to illustrate the methodology by analyzing the most recent vulnerability data from NIST's National Vulnerability Database (NVD). The vulnerabilities were classified in terms of hypervisor functionality, attack type, and attack source. Based on the relative distribution of vulnerabilities in a hypervisor functionality, sample attacks were launched to exploit vulnerabilities in the target hypervisor functionality, and the associated system calls were logged. The gaps in evidence data that is required for fully detecting and reconstructing those attacks were identified, and techniques required to gather missing

evidence were incorporated during subsequent attack runs, essentially performing an iterative process.

Cybersecurity Framework Smart Grid Profile

In FY 2019, engineers from NIST's EL and ITL developed an example Smart Grid implementation of a NIST Cybersecurity Framework Profile. The Smart Grid Profile applies risk management strategies from the Cybersecurity Framework to the smart grid and serves as a foundation for refinements to support new grid architectures. The Profile provides cybersecurity risk management guidance to power system owners and operators by prioritizing cybersecurity activities based on their effectiveness in helping achieve common high-level business objectives for the smart grid. The Profile also provides a list of considerations relevant to the challenges that power system owners and operators may experience as they implement these cybersecurity activities in infrastructures with high concentrations of distributed energy resources. The results were published in NIST Technical Note 2051, *Cybersecurity Framework Smart Grid Profile* [18].

Security Aspects of Electronic Voting

The Help America Vote Act of 2002 (HAVA)[1] encourages the upgrading of voting equipment across the United States and has established the Election Assistance Commission (EAC)[2] and the Technical Guidelines Development Committee (TGDC).[3] NIST chairs the TGDC and provides technical support related to human factors, security, and laboratory accreditation. In FY 2019, NIST developed the Voluntary Voting System Guidelines 2.0 (VVSG 2.0) for national-level voting system standards. VVSG 2.0 is a recommendation from the Technical Guidelines Development Committee (TGDC) to the Election Assistance Commission (EAC) for a voting system standard written to address the next generation of voting equipment.

In FY 2019, NIST provided technical leadership to create an Election Profile of the Cybersecurity Framework in partnership with the Department of Homeland Security (DHS) and the private sector chair of the DHS Sector Coordinating Committee. The Election Profile will serve as a one-stop cybersecurity playbook that matches cybersecurity requirements with operational methodologies across all election processes, from voter registration through election reporting and auditing. The profile can be used by Secretaries of State and state and local election officials to identify and prioritize opportunities to improve their cybersecurity posture. NIST has provided training on the NIST Cybersecurity Framework and profile development and plans to hold future workshops to identify election processes and assets that need protection,

[1] Help America Vote Act of 2002 (HAVA), https://www.law.cornell.edu/wex/hava

[2] U.S. Election Assistance Commission, https://www.eac.gov/

[3] Technical Guidelines Development Committee, https://www.eac.gov/about/technical-guidelines-development-committee/

threats from foreign control of technology vendors, available safeguards, techniques that can detect incidents, and methods to respond and recover.

Secure Blockchain Technologies and Algorithms

While many individuals recognize blockchain technology by its role in enabling *cryptocurrency* (a digital form of currency protected through cryptographic mechanisms), the technology has many applications and can be used to help protect information, enable identity management, and enable purchasing supply chain improvements. In FY 2019, NIST continued to discover and document ways in which the secure use of blockchain technology can enable new applications and capabilities. Publications that NIST developed as technical foundations to advance blockchain research and use included:

- NISTIR 8202, *Blockchain Technology Overview* [19]
- *Smart Contract Federated Identity Management without Third-Party Authentication Services*
- *Augmenting Fiat Currency with an Integrated Managed Cryptocurrency*
- *Implementing a Protocol Native Managed Cryptocurrency*
- *Draft Publication: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*

The team also developed new hardware for a blockchain researcher workbench and an additional blockchain system for deployment. Areas that NIST continues to investigate in the blockchain technology area include:

- Use of a taxonomy for blockchain systems for decentralized identity
- Use of tokens on blockchain systems
- Creation of tools to enable blockchain technology research
- Use of blockchain technology to publicly generate trustworthy random numbers
- Development of an architecture to enable the creation of managed cryptocurrencies that incorporate security features from consensus currencies
- Application of a methodology for securely storing and monitoring the use of federally owned crypto-assets on existing cryptocurrency systems
- Continued exploration of emerging topics and newly developed and released blockchain systems

CREDIT: iStock / alexsl

FOCUS AREA 5: IMPROVING CYBERSECURITY AWARENESS, TRAINING, AND EDUCATION AND WORKFORCE DEVELOPMENT

People are often the most underappreciated ingredient in the people, process, and technology formula that determines an organization's readiness to understand and deal with cybersecurity challenges. This includes gaps in user and provider awareness about how to access cybersecurity guidelines and tools that apply to their own operations and environments along with a shortage of people who have the needed cybersecurity education, training, and experience.

National Initiative for Cybersecurity Education (NICE)

Led by NIST, NICE seeks to equip, promote, and energize a robust network of organizations that address cybersecurity education, training, and workforce development. In FY 2019, the NICE program celebrated its 10th anniversary. Efforts to achieve this goal include: 1) accelerating learning and skills development, 2) nurturing a diverse learning community, and 3) guiding career development and workforce planning to achieve each of the objectives identified in the *NICE Cybersecurity Workforce*

Framework (see https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center) [20].

Some of the key accomplishments for NICE during FY 2019 include:

- Growth in the National Centers of Academic Excellence in Cybersecurity – NIST and NICE support the National Centers of Academic Excellence (CAE) in Cybersecurity through a grant that funds the annual CAE Symposium held in conjunction with the annual NICE Conference and Expo. During FY 2019, the number of CAE institutions grew to 312, with 60 new CAE designations occurring during the NICE Conference and Expo. NICE also supports the CAE community through participation in and travel to the annual CAE Executive Leadership Forum. The National Security Agency and DHS co-lead the CAE Program.
- NICE Cybersecurity Workforce Framework Promotion and Alignment – Executive Order (EO) 13870, *America's Cybersecurity Workforce*, has continued to increase awareness about the NICE Framework and encouraging its adoption by government, industry, and academia [21]. The EO requires an extension of the NICE Framework to federal contractors that provide cybersecurity or IT services to the Federal Government and encourages voluntary adoption by nonfederal entities. NIST continues to learn about applications and uses of the NICE Framework across public and private sectors and expects to use that experience and feedback to improve the NICE Framework during FY 2020.
- Public Conferences – The NICE team prepared for the 10th Annual NICE Conference and Expo and the 5th Annual NICE K12 Cybersecurity Education Conference. The broader NICE Conference will be held in Phoenix, Arizona in early FY 2020. The next NICE K12 Cybersecurity Education Conference, to be held in Garden Grove, California, will support school teachers, administrators, non-profit organizations, and others who mentor children and youth interested in cybersecurity as a career.
- International Engagement – NICE convenes bi-monthly meetings of Five Eyes partner countries (Australia, Canada, New Zealand, the United Kingdom, and the United States) to learn about each country's respective initiatives and challenges in cybersecurity education and workforce development. NICE also actively participates in a working group on Cyber Culture and Skills of the Global Forum for Cyber Expertise (GFCE). NICE staff presented on the topic of "Workforce Development Frameworks" at the GFCE Annual Meeting in Ethiopia. NICE also coordinated a four-day International Workshop on Cybersecurity Education and Workforce Development Capacity Building in Germany.

Increasing Awareness of Cybersecurity Resources

A major element of NIST's work in information security involves the publication of cybersecurity and privacy documents as well as engagement with public and private-sector communities. FY 2019 activities to increase and improve awareness included:

- The Computer Security Resource Center (CSRC), one of the most visited websites at NIST, provides a central resource for NIST cybersecurity and privacy publications, standards, and guidelines. The purpose of the CSRC is to encourage the broad sharing of information security tools and practices, provide a resource for information security standards and guidelines, and identify and link key security resources to support the industry. In FY 2019, the CSRC was updated to provide an enhanced search capability and a more consistent and modernized user interface.
- Cybersecurity for Small Businesses supports the small and medium-sized businesses (SMBs) that represent approximately 95% of all businesses and are often considered to be the backbone of the U.S. economy.[4] Typically faced with limited budgets, SMBs need practical resources that enable them to understand and cost-effectively address their cybersecurity risks. NIST has been working on behalf of SMBs for many years, together with interagency and industry partners and collaborators. The NIST Small Business Cybersecurity Act codified the Institute's focus on small businesses. Specifically, the statute directed NIST to "disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks." In FY 2018, the NIST Small Business Outreach Program began updating the Small Business Cybersecurity Corner website to make resources easier to find and use (https://www.nist.gov/itl/smallbusinesscyber). In FY 2019, those training materials and accompanying resources have been expanded, based on cybersecurity resources and feedback received from NIST's federal partners and the public.
- The Federal Computer Security Program Managers (FCSM) Forum is an important component of improving cybersecurity awareness, training, and workforce development. FCSM is an informal NIST-sponsored group that promotes the sharing of system security information among U.S. federal, state, and higher education organizations. In FY 2019, FCSM conducted three half-day quarterly meetings and hosted a annual two-day off-site meeting to discuss current issues and items of interest with those responsible for protecting non-national security systems.

[4] The most recent data from the U.S. Census Bureau, Business Dynamics Statistics (BDS) Firm and Establishment Data Tables, shows that 95.52 % of "firms" have between 1 and 49 employees and could be considered by many to be SMBs.

Advancing Cybersecurity Usability

ITL's Visualization and Usability Group performs research to develop user-centered measurement and evaluation methods, guidelines, and standards by applying human factors, cognitive science, user-centered designs, and usability principles to improve interactions between humans and systems. In FY 2019, notable usability projects included:

- Human Factors in Smart Home Technologies – NIST conducted a one-day workshop entitled "Human Factors in Smart Home Technologies." Inspired by the team's smart home research, the workshop addressed the human aspects of smart home devices, including usability, user perceptions, and end-user privacy and security considerations. Invited speakers from industry, academia, and the government provided their perspectives via presentations and a moderated panel. The attendees also had the opportunity to influence NIST's future research direction in this area by voicing their opinions, challenges, and ideas during breakout sessions.

- Rating Human Phishing Message Detection Difficulty – NIST also developed the "Phish Scale" as a tool 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 to rate the difficulty of their organization's phishing exercises and explain associated click rates. Research results were shared with industry, academia, and government representatives at multiple security forums and will be published in the Journal of Cybersecurity.

- Understanding Youth Cybersecurity Practices and Perceptions – Cybersecurity for young people remains an important area of study for NIST. In FY 2019, NIST completed a study to understand a child's password practices and perceptions. Children use technology from a very young age and often have to authenticate themselves. Yet very little attention has been paid to designing authentication methods specifically for this particular target group. The usual practice is to deploy the ubiquitous password, and this might well be a suboptimal choice. Designing authentication for children requires acknowledgement of child-specific developmental challenges related to literacy, cognitive abilities, and differing developmental stages. Understanding current security practices is essential to delivering insights that can inform the development of child-centered authentication mechanisms and processes. NIST conducted a systematic review of twenty years of research related to children and authentication, noting a research gap regarding the creation and use of passwords. This finding led to a survey of U.S. school children to gain insights into their current password usage and behaviors. The team analyzed password survey responses collected from more than 1500 students in grades 3 to 12. The results were published in the Journal of Cybersecurity. The ultimate goal of the research is the development of useful guidance to help educators, parents, and youth understand the best practices for passwords and online security and privacy.

CREDIT: Shutterstock / nmedia

FOCUS AREA 6: ENHANCING IDENTITY AND ACCESS MANAGEMENT

Properly managing access to systems, processes, and information is central to managing cybersecurity risks and a priority for NIST's cybersecurity and privacy program. NIST engages and collaborates with standards bodies and consortia such as the International Organization for Standardization (ISO),[5] the Internet Engineering Task Force (IETF),[6] the Fast IDentity Online (FIDO) Alliance,[7] the Open Identity Federation (OIF), and the Kantara Initiative[8] to document and advance the various methods for ensuring reliable and secure identity and access management. NIST began the development of the Identity and Access Management Resource Center in FY 2019. This virtual resource center was designed to share NIST's efforts to strengthen the security, privacy, usability, and interoperability of identity and access management solutions and includes convenient links and details relative to NIST identity projects across the entire organization.

Digital Identity Guidelines

Federal agencies and industry have had over two years of experience in assimilating, adopting, and implementing the controls and requirements of the four-volume set of digital identity publications: NIST Special Publication (SP) 800-63-3, *Digital Identity*

5 International Organization for Standardization (ISO), https://www.iso.org/home.html

6 Internet Engineering Task Force (IETF), https://www.ietf.org/about/

7 Fast IDentity Online Alliance (FIDO), https://fidoalliance.org/

8 Kantara Initiative, https://kantarainitiative.org/

Guidelines; SP 800-63A, *Enrollment and Identity Proofing;* SP 800-63B, *Authentication and Lifecycle Management*; and, SP 800-63C, *Federation and Assertions* [22]. SP 800-63-3 represented a major update to the previous SP 800-63-2 standard and advanced new approaches for componentization, assurance levels, authenticators, federation, and privacy considerations. There has been widespread interest, analysis, and adoption by industry and international standards organizations of SP 800-63-3 for its concepts and guidance, control requirements, and application of the Risk Management Framework to identity management systems. During FY 2019, NIST has been working closely with federal agencies and industry for the implementation of the standard. Questions and issues are publicly posted on NIST Pages (see https://pages.nist.gov/800-63-FAQ/) and as open issues on GitHub (see https://github.com/usnistgov/800-63-3/issues).

OMB Policy Memorandum M-19-17 updated federal identity, credentials, and access management policy and provided direction for federal agencies to enhance associated capabilities [23]. In response, NIST established the Identity and Access Management (IAM) Resource Center, which provides information and resources for NIST IAM[9] activities. The IAM Resource Center includes a roadmap of major NIST projects and activities. The roadmap presents NIST plans to update SP 800-63-3 in order to build on the feedback already received, starting with a formal request for comments in the third quarter of FY 2020.

M-19-17 assigned to NIST the responsibility for developing conformance criteria for the accreditation of products and services to meet designated levels of assurance in SP 800-63-3. In response, NIST explored various conformance regimes that might be leveraged so that the conformance criteria could be developed in the most appropriate fashion. The conformance criteria present all normative requirements and controls of SP 800-63-3 by designated assurance level. These include conformance assessment objectives for each criterion, recommended methods for determining conformity with the requirements, and supplemental guidance to assist implementers and assessors to achieve and determine conformity. The conformance criteria are intended for federal agencies and industry service providers for their specific implementations and risk and security assessments under FISMA.

Personal Identity Verification (PIV)

As required by Homeland Security Presidential Directive 12, NIST developed and maintains the FIPS for personal identity verification (PIV) of federal employees and contractors (FIPS 201). In FY 2019, NIST initiated the revision of FIPS 201 with the goals of incorporating the new or changing business requirements of federal departments and agencies, adapting to changes in the environment and technology, and aligning with M-19-17. The revision activities began with a business requirement meeting to engage with federal stakeholders about the revision goals. Based on the engagement, NIST aims to expand the set of PIV authenticators beyond the current practices (including

[9] NIST Identity and Access Management, https://www.nist.gov/topics/identity-access-management

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. The PIV team actively worked on drafting a candidate public draft of the updated FIPS 201-3 while continuing outreach to federal stakeholders.

CREDIT: Shutterstock / metamorworks

FOCUS AREA 7: BOLSTERING COMMUNICATIONS AND INFRASTRUCTURE PROTECTION

NIST works with industry to develop the measurement science and standards necessary to ensure the robustness, scalability, and security of important infastructures, 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. The NIST staff uses these insights to guide the design, analysis, and standardization of new technologies aimed at improving the robustness and reliability of the global communications infrastructure.

Much of the research and industry collaboration occurs at NIST's National Cybersecurity Center of Excellence (NCCoE). As shown in Figure 2 below and in the accomplishments described in this focus area, the center represents the significant benefit of government-industry partnership.

Figure 2: Selected Impacts of NCCoE

Securing Cellular and Mobile Technologies

Some of the most exciting advances in technology are those involving mobile networking and communications. Cellular technologies are increasing in bandwidth capabilities as they evolve from 3rd generation (3G) to 4th generation (4G), Long Term Evolution (LTE) and, 5th generation (5G) technologies. The mobile technologies that leverage this infrastructure are becoming more powerful and offering more services to consumers. NIST is working to ensure that these technologies have the necessary security and privacy capabilities to be reliable and trustworthy.

In FY 2019, NIST continued its participation in the 3rd Generation Partnership Project (3GPP) that unites telecommunications standard development organizations in maintaining and advancing cellular telecommunications technologies (including radio access and core network and service capabilities) to enable and improve mobile telecommunications. 3GPP specifications and studies are contribution-driven by member companies in Working Groups and at the Technical Specification Group level. NIST participation in 3GPP activities helps to ensure compatibility for legacy technology and helps in the development of standards for the next generation (e.g., 5G) cellular technologies.

NIST published a practice guide–SP 1800-21, *Mobile Device Security: Corporate-owned Personally-Enabled* (COPE)–for public comment [24]. The goal of the COPE project was to provide an example solution that demonstrates how organizations can use a standards-based approach and commercially available technologies to meet their security needs for using mobile devices to access enterprise resources. Usability, privacy, and regulatory requirements influence which mobile security technologies and security controls are going to be well-suited to meet the needs of an organization's mobility program. The sample solution provides the details of tools for an enterprise mobility management (EMM) capability located on-premises, including mobile threat defense (MTD), mobile threat intelligence (MTI), application vetting, secure boot/image authentication, and virtual private network (VPN) services. (See https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/corporate-owned-personally-enabled.)

Advancing 5G Security

As the next generation of mobile broadband technology—the 5th Generation, or 5G—is deployed in our nation and across the world, there is great promise of positive change in the way humans and machines communicate, operate, and interact in the physical and virtual world. With cellular technology becoming the primary way that devices are connected, it is imperative for organizations to understand and address the risks associated with the use of these technologies. As industry embarks on ubiquitous 5G deployments, there are opportunities to take advantage of the various cybersecurity technologies and capabilities that are available today. 5G introduces the concept of a service-based architecture for the first time in cellular networks. This design has fundamental impacts on the way network services are created and how the individual network functions communicate. Not only is the core network decomposed into smaller functional elements, but the communication between these elements is also expected to be more flexible—routed via a common service bus and deployed using virtualization technologies. It is envisioned that 5G network components are deployed on a hyper-scalable, containerized, and virtualized infrastructure. While this is not the only approach for 5G deployments, this infrastructure is a fundamental building block of 5G that operators and manufacturers can adopt to meet the customers' demands of modern use cases. Secure deployment of the core network and radio access network services on cloud-like infrastructures constitutes a foundational element of both commercial and private 5G networks.

In FY 2019, NIST hosted a public workshop on 5G cybersecurity at the NCCoE. The purpose of the workshop was to explore the practical and implementable cybersecurity capabilities delivered by 5G systems, identify existing industry recommended practices for securing the supporting infrastructure and technologies, and understand the potential opportunities and challenges that affect the 5G evolution. The findings from this workshop will inform the development of potential NCCoE demonstration projects to leverage 5G cybersecurity capabilities and supporting technologies to protect the cellular communications network and secure the core 5G underlying infrastructure and services.

During the workshop, NIST introduced some notional ideas of a high-level reference architecture, supporting components of 5G deployments, and a proposed preliminary approach for gathering existing cybersecurity guidance to develop practical practices that can be applied as potential NCCoE demonstration projects.

National Public Safety Broadband Network (NPSBN)

Federal statutes direct NIST to conduct research and development that support the acceleration and advancement of a nationwide broadband network that will help police, firefighters, emergency medical service professionals, and other public safety officials stay safe and do their jobs. Having a common and reliable National Public Safety Broadband Network (NPSBN) enables these officials to effectively communicate and conduct their missions. In FY 2019, NIST continued to research and advance methods and guidelines for this community, including:

- Publication of draft NISTIR 8196, *Security Analysis of First Responder Mobile and Wearable Devices*, which reviews the current and potential use cases of these mobile and wearable devices by first responders and analyzes them from a cybersecurity perspective [25]. The goals of this analysis were to enable industry to design and produce more secure public safety devices and to assist jurisdictions in identifying security objectives and selecting secure devices.
- Collaboration with the NIST Public Safety Communications Research (PSCR) Division's prize challenge. Contestants explored whether mobile Subscriber Identity Module (SIM) cards could be used as storage containers for public safety mobile application credentials. PSCR reached out to providers globally to participate in a competition aimed at improving public safety operations through innovative improvements to SIM card functionality. The goals of this research were to raise awareness of the need for convenient, standards-based, two-factor authentication for emergency responders while demonstrating an innovative approach to authentication that could lead to future innovations.
- NCCoE released a second draft of NIST Cybersecurity Practice Guide SP 1800-13, *Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders* [26]. This revision of the guide was updated at the request of the public safety community to incorporate iOS version 12.

Zero Trust Architecture

Zero Trust is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan the 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., local area networks versus the internet). Authentication and authorization (both user and device) are discrete functions performed before a session with an enterprise resource

is established. Zero trust is a response to enterprise network trends that include 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 has published Draft SP 800-207, *Zero Trust Architecture*, which discusses the core logical components that make up a zero trust architecture (ZTA) network strategy [27]. Draft SP 800-207 contains a definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

Improving Security Hygiene

There are a relatively small number of root causes for many data breaches, malware infections, and other security incidents. Implementing a few simple practices can address those root causes to prevent many incidents from occurring and to lower the potential impact of incidents that still occur. In other words, security hygiene practices make it harder for attackers to succeed and reduces the damage that they can cause. Unfortunately, security hygiene is easier said than done. For example, IT professionals have known for decades that patching software (e.g., operating systems, applications, and the like) eliminates known vulnerabilities. Though there is widespread recognition that patching can be incredibly effective at mitigating security risk, patching is often resource-intensive, and the act of patching itself can reduce system and service availability.

Installing software updates (i.e., patching) is a particularly important component of cyber hygiene, but existing tools are insufficient for many environments and situations. For example, many organizations lack tools to help them measure and assess the effectiveness and timeliness of their patching efforts. Many organizations also struggle to prioritize patching efforts, test patches before deployment, and adhere to policies for how quickly patches need to be applied in different situations. How, when, and what to patch can be difficult decisions for any organization. Each organization must balance security with mission impact and business objectives and figure out their risk tolerance for each. Recent cybersecurity attacks have highlighted the dangers of having equipment that has not been patched. Even with recent events and the historical attacks that have been successfully carried out due to unpatched systems, patching remains a problem.

The NCCoE launched a project to demonstrate an approach for improving enterprise patching practices for general IT systems. In this project, commercial and open-source tools will be used to address the most challenging aspects of patching, including system characterization and prioritization, patch testing, and patch implementation tracking and verification. These tools are accompanied by actionable, prescriptive guidance on establishing policies and processes for the entire patching life cycle. For example, roles and responsibilities are defined for all affected personnel, and a playbook is established with rapid mitigation actions for destructive malware outbreaks that organizations can tactically execute in the first 30 days as well as recommendations that can be implemented strategically beyond 30 days. This project has resulted in

the NIST Cybersecurity Practice Guide, *Critical Cybersecurity Hygiene: Patching The Enterprise*, that will be released in FY 2020. This report provides practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Secure Inter-Domain Routing (SIDR)

Most of the routing infrastructure that underpins the internet currently lacks basic security services. In most cases, internet traffic must transit multiple networks before reaching its destination. Each network implicitly trusts other networks to provide, via the Border Gateway Protocol (BGP), the accurate information necessary to correctly route traffic across the internet. When that information is inaccurate, traffic will take inefficient paths through the internet, potentially arriving at malicious sites that masquerade as legitimate destinations or never arriving at its intended destination at all.

In FY 2019, NIST researchers collaborated at the NCCoE to demonstrate the ability of a technique known as BGP route origin validation (ROV) to protect against route hijacking. This project culminated in an NCCoE practice guide, NIST SP 1800-14, *Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation,* which provided an example implementation that demonstrated the use of BGP ROV in realistic deployment scenarios; developed detailed deployment guidance; addressed implementation and use issues; and generated best practices and lessons learned [28]. This resource is intended to improve the security and stability of the global internet by allowing networks to verify the validity of BGP routing information and strengthen the security and stability of traffic flowing across the global internet—benefitting all organizations and individuals that use and rely on it.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a cryptographic protocol that is designed to provide privacy and data integrity between two or more communicating computer applications over a computer network. TLS is widely used in many common applications, including web browsing, email, instant messaging, and Voice over Internet Protocol (VoIP). Websites often use TLS to secure communications between servers and web browsers.

In FY 2019, the NCCoE initiated a project that uses commercially available technologies to demonstrate how medium and large enterprises that rely on Transport Layer Security (TLS) can secure both customer-facing and internal applications to manage TLS server certificates better by:

- Defining operational and security policies and identifying roles and responsibilities;
- Establishing comprehensive certificate inventories and ownership tracking;
- Conducting a continuous monitoring of certificate operational and security status;

- Automating certificate management to minimize human error and maximize efficiency on a large scale; and
- Enabling rapid migration to new certificates and keys when cryptographic mechanisms are found to be weak, compromised, or vulnerable.

The project will result in actionable guidance to help enterprises establish and implement a TLS server certificate management program.

CREDIT: Shutterstock / jamesteohart

FOCUS AREA 8: SECURING EMERGING TECHNOLOGIES

NIST has maintained a long-standing commitment to advancing innovation and to supporting cybersecurity and privacy research in emerging technologies and priorities, such as artificial intelligence and the Internet of Things (IoT). With a dedicated technical staff, one-of-a-kind facilities, and NIST's trusted, objective, non-regulatory role, NIST is well-positioned to help the Nation and its partners advance in these promising areas.

Cybersecurity for the Internet of Things (IoT)

NIST's Cybersecurity for the Internet of Things (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 of the NIST IoT program in FY 2019 included:

- Publication of the Final NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, which provides guidance for federal agencies and other organizations to better understand and manage the risks associated with individual IoT devices throughout the life cycles of those devices [6]. It addresses three high-level goals for risk mitigation: device security, data

security, and individual privacy. This introductory report provides the foundation for a planned series of publications on more specific aspects of this topic.

- Publication of Draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* [29]. This NISTIR defines a baseline of cybersecurity features that manufacturers may voluntarily adopt for the IoT devices that they produce. It also provides information on how manufacturers can identify and implement features beyond the baseline that are most appropriate for their customers.
- Publication of Draft NISTIR 8267, *Security Review of Consumer Home Internet of Things (IoT) Products*, which presents the results of technical assessments on the security features of various "smart" products (e.g., smart light bulbs, security cameras, and doorbells) [30]. The report provides recommendations, information on the observations of the devices' security features, current practices, and the means by which these current practices could be improved. These technical assessments will help the NCCoE better address consumer home IoT security in a holistic manner in future projects.

Federal Engagement for Artificial Intelligence

As artificial intelligence (AI) is rapidly transforming our world, remarkable surges in AI capabilities have led to a number of innovations. New AI-enabled systems are revolutionizing everything from commerce and healthcare to transportation and cybersecurity. Because AI has the potential to impact nearly all aspects of our society including our economy, AI must be developed in a trustworthy manner to ensure reliability, safety, and accuracy.

Drawing upon NIST's long-standing reputation for cultivating trust in technology, the NIST staff is helping to ensure the public trust of rapidly evolving technologies, including the development of rigorous and scientific testing that ensures safe and trustworthy AI. Our progress includes:

- Participation in interagency efforts to further innovate AI. NIST Director and Undersecretary of Commerce for Standards and Technology Walter Copan serves on the White House Select Committee on Artificial Intelligence. Charles Romine, the Director of NIST's ITL, serves on the Machine Learning and AI Subcommittee.
- Creation of a plan in response to Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*, for prioritizing federal agency engagement in the development of standards for AI [31]. The plan recommends that the Federal Government "commit to deeper, consistent, long-term engagement" in activities to help the United States speed the pace of reliable, robust, and trustworthy AI technology development; bolster AI standards-related knowledge, leadership, and coordination among agencies that develop or use AI; promote focused research on

the trustworthiness of AI systems; support and expand public-private partnerships; and engage with international parties.

- NIST published draft NISTIR 8269, *A Taxonomy and Terminology of Adversarial Machine Learning,* in FY 2019 as a step toward securing applications of AI, specifically adversarial machine learning (AML), and features a taxonomy of concepts and terminologies [32]. This NISTIR can inform future standards and best practices for assessing and managing machine learning security by establishing a common language and understanding of the rapidly developing AML landscape.

NIST is also supporting fundamental research to measure and enhance the security and explainability of AI systems and advancing the application of AI to NIST metrology problems by bolstering AI expertise at NIST and enabling NIST scientists to draw routinely on machine learning and AI tools to gain a deeper insight into their research. NIST launched the AI Visiting Fellow program, which brings nationally recognized leaders in AI and machine learning to NIST to share their knowledge and experience and provide technical support.

NIST research in AI is focused on how to measure and enhance the security and trustworthiness of AI systems. This includes participation in the development of international standards that ensure innovation, public trust, and confidence in systems that use AI technologies. In addition, NIST is applying AI to measurement problems to gain deeper insight into the research itself as well as to better understand AI's capabilities and limitations. In FY 2019, the NCCoE also began developing a testbed to research and develop metrics and best practices to assess the vulnerabilities of AI models.

CREDIT: Shutterstock / kentoh

FOCUS AREA 9: ADVANCING SECURITY TEST AND MEASUREMENT TOOLS

Federal agencies, industry, and the public rely on many elements of software and technology for the protection of information and communications used in electronic commerce, the critical infrastructure, and other application areas. This reliance depends on the effective measurement and conformance testing of the standards being applied.

In FY 2019, NIST continued to create reference data, offer guidance, and participate in international engagement for the development of flexible, open standards. These efforts will be continued in FY 2020 as NIST seeks to improve the interoperability, broad acceptance, and adoption of security automation solutions to address the current and future security challenges. In turn, this will create opportunities for innovation.

Automated Combinatorial Testing

As important as software is to modern, complex information and technology systems, that complexity makes it difficult and expensive to conduct adequate vulnerability testing in a timely manner. Engineers often encounter security failures that result from unexpected interactions among components. If all faults in a system can be triggered by applying test methods that combine a known number of parameters, then testing all possible combinations of those parameters with a practical number of tests can provide strong fault detection efficiency. These methods are being applied to software

and hardware testing for reliability, safety, and security.[10] NIST's focus is on empirical test results and their impact on real-world problems. In FY 2019, NIST was able to advance such testing by developing and demonstrating methods for generating very large (> 2000 variables) test arrays. This tool is being applied by industry to evaluate the quality of their test suites for commercial products. NIST also conducted a joint project with Idaho National Labs and Virginia Commonwealth University to demonstrate combinatorial methods for software assurance in reactor safety systems as well as a similar project with the National Aeronautics and Space Administration (NASA) to demonstrate combinatorial coverage measurement for spacecraft software assurance.

National Vulnerability Database (NVD)

How does a system administrator know if some of the hardware or software in their systems contain vulnerabilities? Chances are that they utilize information that is freely available from the NVD. The NVD is a comprehensive cybersecurity vulnerability database that tracks vulnerability discovery trends over time, enabling users to assess changes in vulnerability discovery rates within specific products or types of vulnerabilities. The NVD includes databases of security configuration checklists for the National Checklist Program (NCP), which is comprised of listings of publicly known software flaws, product names, and impact metrics.

NVD data is represented using the Secure Content Automation Protocol (SCAP) specifications. The use of SCAP data by the commercial security products deployed in thousands of organizations worldwide has extended NVD's effective reach.

The graphic below demonstrates the significant impact of the NVD and why it is a critical element of NIST's advancement of information security testing, measurement science, and conformance. NIST staff have worked diligently to significantly increase the information available from the NVD repositories, expand the automated mechanisms to access that information, and provide timely evaluations of new and evolving vulnerability data. The numbers reflected in this chart illustrate these improvements, such as an increase of 556% of modified Common Vulnerability Enumeration (CVE) analysis compared to 2018, 160% increase in the listed Common Platform Enumeration (CPE) platforms, and considerable reduction of the historical backlog of CVEs waiting to be processed.

[10] Automated Combinatorial Testing for Software, https://csrc.nist.gov/projects/automated-combinatorial-testing-for-software

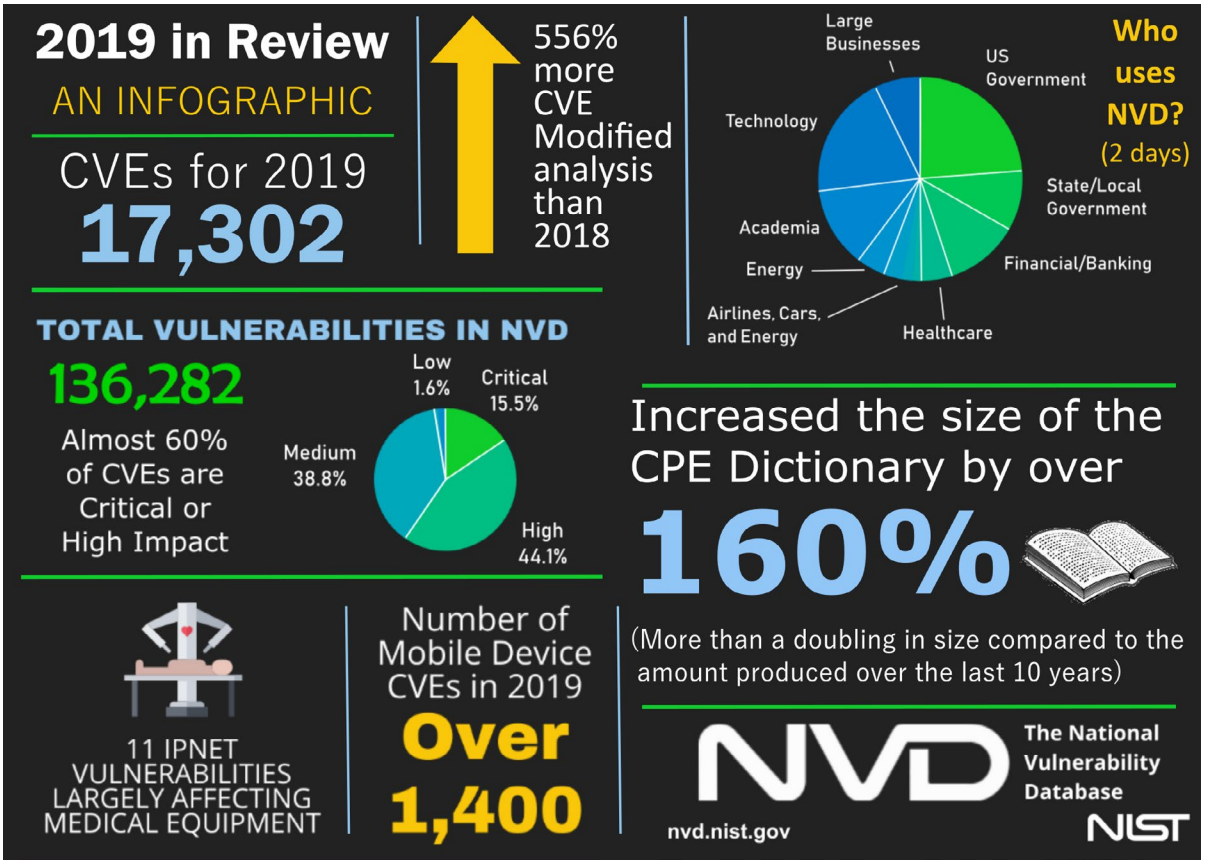


Figure 3: Selected FY 2019 NVD Accomplishments

Several strategies to gain efficiencies, provide better value, and meet future demands are planned for the NVD in FY 2020. Improvements in tools and workflow for the analysts are continuously being developed, and the team intends to implement the allowlisting of CVE Naming Authorities (CNAs). This would allow some CNAs to provide their own analyses of CVEs, and after internal review, their scores could automatically be accepted into the NVD. This process will be further described in NISTIR 8246, *National Vulnerability Database (NVD) Metadata Submission Guidelines for Common Vulnerabilities and Exposures (CVE) Numbering Authorities (CNAs) and Authorized Data Publishers*, which is expected to be published in FY 2020. The team also plans to implement a vulnerability ontology (commonly referred to as "vulntology"). This ontology approach will be published for public comment in FY 2020 and used to determine whether natural language processing (i.e., AI) will be useful in the future analyses of CVEs.

Open Security Controls Assessment Language (OSCAL)

Today, concepts like security controls and profiles are largely represented in proprietary ways, making it more difficult for many organizations to move forward as quickly as they need to in order to take advantage of these approaches. Organizations also often struggle with information systems that have many different components. To help address these problems, NIST is collaborating with industry to develop the Open Security

Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in eXtensible Markup Language (XML), JavaScript Object Notation (JSON), and YAML Ain't Markup Language (YAML). These formats provide machine-readable representations of control catalogs, control baselines, system security plans, assessment plans, and results. In FY 2019, NIST continued to develop approaches for security planning and measurement through the application of the Cybersecurity Framework for assessments and assessment results.

Cyber Risk Analytics

This project promotes technical solutions that enable organizations to bridge diverse, new, and existing data sets to advance the analysis of cyber risks and enhance the ability to report trends. The goal is to enable information sharing among risk owners about historical, current, and future cyber risk conditions. NIST is leveraging their past and present efforts such as a data repository for cyber incident analysis, predictive analytics and strategic analysis on threat coverage, and prioritization and gap identification. In FY 2019, the program developed methodologies and tools that could be used for developing a Collaborative Cyber Incident Data and Analysis Repository (CIDAR)[11] that will combine data from multiple databases and showcase opportunities for visualizing patterns and trends in cyber-related incidents. The methodologies developed also included the automation of new data ingestion and predictive functions to match cyber incident entries between data sets.

Computer Forensic Tool Testing (CFTT)

The Computer Forensics Tool Testing Program (CFTT) is a project of ITL's Software and Systems Division (SSD) and is supported by the Special Programs Office and DHS. In FY 2019, several key advances were made to help address a critical need in the law enforcement community to ensure the reliability of computer forensic tools.

- Specifications and Testing – A new test specification for mobile devices was developed: *Mobile Device Forensic Tool Specification, Test Assertion, and Test Cases*. The CFTT project partnered with DHS to test numerous digital forensic tools for disk imaging, write-blocking, string searching, windows registry, and mobile device acquisition, resulting in 23 published reports.
- Federated Testing – Federated testing was developed to enable third parties to use the NIST testing methodology in their own labs and produce standardized test reports. In FY 2019, Federated Testing v4 was updated to provide modules for disk imaging tools, forensic string search tools, hardware write blockers, and mobile forensic tools.

[11] *Enhancing Resilience Through Cyber Incident Data Sharing and Analysis*, https://www.cisa.gov/sites/default/files/publications/Overcoming%20Perceived%20Obstacles%20White%20Paper_1.pdf

- Computer Forensic Reference Data Sets (CFReDS) – The CFReDS is a repository of various documented sets of digital evidence. In FY 2019, CFReDS was updated to include five Joint Test Action Group (JTAG) and nine Chip-Off mobile device binary images, string search test data for use with Federated Testing 4.0 and later, and 19 drone forensic images.
- Forensics Tool Catalog – The Forensics Tool Catalog is a web-based community-sourced catalog of forensic tools aided by a taxonomy of forensic tools. The Tool Catalog grew by two functionalities (Live Response and Incident Response Forensic Tracking and Reporting) and 63 new tool entries for a total of 315 tools in FY 2019.

National Software Reference Library (NSRL)

The NSRL is designed to collect software from various sources and incorporate the file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry to review computer files by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations. The NSRL also provides a research environment to promote the development of new forensics techniques and other applications in computer science.

In FY 2019, the NSRL published four releases of software metadata and enlarged the collection to contain a combined total of 544 million files from 30,000 microcomputer applications; 169,000 mobile device applications; and 3,700 gaming platform applications. The NSRL was also expanded to include applications that were distributed through gaming platforms and the profiles obtained from installing and updating common operating systems.

CONCLUSION

We are very proud of our accomplishments and enjoy sharing the culmination of our work with you each year. Our commitment to cultivating trust in information and the technology that drives the development and handling of that information is one of our top priorities, and we thank you for your continued support in these endeavors.

As always, NIST welcomes all suggestions for how we can improve our cybersecurity work to better serve the public and private sectors. We also warmly welcome you to join us in the future as we pick up the pace and work together.

REFERENCES

[1] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[3] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[4] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[5] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[6] Boeckl KR, Fagan MJ, Fisher WM, Lefkovitz NB, Megas KN, Nadeau EM, Piccarreta BM, Gabel O'Rourke D, Scarfone KA (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[7] Stouffer KA, Zimmerman T, Tang C, Lubell J, Cichonski JA, McCarthy J (2019) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183, Includes updates as of May 20, 2019. https://doi.org/10.6028/NIST.IR.8183

[8] Keller N, Quinn S, Scarfone K, Smith M, Johnson V. (2020). National Cybersecurity Online Informative References (OLIR) Program: Guidelines for OLIR Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal or Interagency Report (NISTIR) 8278. https://doi.org/10.6028/NIST.IR.8278-draft

[9] Barrett M, Keller N, Quinn S, Smith M. (2019). Cybersecurity Framework Online Informative References (OLIR) Submissions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal or Interagency Report (NISTIR) 8204. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8204.pdf

[10] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[11] Ross RS, Dempsey KL, Pillitteri VY (2018) Assessing Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A. https://doi.org/10.6028/NIST.SP.800-171A

[12] Ross RS, Pillitteri VY, Guissanie G, Wagner R, Graubart R, Bodeau D (2019) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-171B. https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf

[13] Dodson D, Souppaya M, Scarfone K. (2020). Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) (National Institute of Standards and Technology, Gaithersburg, MD), https://doi.org/10.6028/NIST.CSWP.04232020

[14] Paulsen C, Winkler K, Boyens J, Ng J, Gimbi J (2020). Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal or Interagency Report (NISTIR) 8272. https://doi.org/10.6028/NIST.IR.8272-draft

[15] Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2020). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal or Interagency Report (NISTIR) 8276. https://doi.org/10.6028/NIST.IR.8276-draft

[16] Alagic G, Alperin-Sheriff J, Apon D, Cooper DA, Dang QH, Miller CA, Moody D, Peralta R, Perlner RA, Robinson A, Smith-Tone D, Liu Y-K (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240. https://doi.org/10.6028/NIST.IR.8240

[17] Turan MS, McKay KA, Çalık Ç, Chang D, Bassham L. Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process (2019). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8268. https://doi.org/10.6028/NIST.IR.8268

[18] Marron JA, Gopstein AM, Bartol N, Feldman V (2019) Cybersecurity Framework Smart Grid Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 2051. https://doi.org/10.6028/NIST.TN.2051

[19] Yaga DJ, Mell PM, Roby N, Scarfone KA (2018) Blockchain Technology Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8202. https://doi.org/10.6028/NIST.IR.8202

[20] Newhouse WD, Scribner B, Keith S. Witte GA (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[21] Executive Order 13870 (2019) America's Cybersecurity Workforce. (The White House, Washington, DC), Federal Register Volume 84, Issue 90 (May 9, 2019). https://www.govinfo.gov/app/details/FR-2019-05-09/2019-09750

[22] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[23] Office of Management and Budget (2019) M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[24] Franklin JM, Howell G, Boeckl K, Lefkovitz N, Nadeau E, Shariati D, ... Peck M (2019). Mobile Device Security Corporate-Owned Personally-Enabled (COPE). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-21. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mdse-nist-sp1800-21-draft.pdf

[25] Franklin J, Howell G, Ledgerwood S, Griffith J. (2018). Security Analysis of First Responder Mobile and Wearable Devices. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal or Interagency Report (NISTIR) 8196. https://doi.org/10.6028/NIST.IR.8196-draft

[26] Fisher W, Grassi P, Dog S, Jha S, Kim W, McCorkill T, ... Barker W. (2019). Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Special Publication (SP) 1800-13. https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

[27] Rose S, Borchert O, Mitchell S, Connelly S. (2019). Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207-draft2

[28] Haag WA, Jr, Montgomery DC, Barker WC, Tan A (2019) Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-14. https://doi.org/10.6028/NIST.SP.1800-14

[29] Fagan M, Megas K, Scarfone K, Smith M. (2019). Core Cybersecurity Feature Baseline For Securable Iot Devices: A Starting Point For Iot Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Internal or Interagency Report (NISTIR) 8259. https://doi.org/10.6028/NIST.IR.8259-draft2

[30] Fagan M, Yang M, Tan A, Randolph L, Scarfone K. (2019). Security Review of Consumer Home Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Internal or Interagency Report (NISTIR) 8267. https://doi.org/10.6028/NIST.IR.8267-draft

[31] Executive Order 13859 (2019) Maintaining American Leadership in Artificial Intelligence. (The White House, Washington, DC), DCPD- 201900073, February 11, 2019. https://www.govinfo.gov/app/details/DCPD-201900073

[32] Tabassi, E., Burns, K. J., Hadjimichael, M., Molina-Markham, A. D., & Sexton, J. T. (2019). A Taxonomy and Terminology of Adversarial Machine Learning. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8269. https://doi.org/10.6028/NIST.IR.8269-draft

ACRONYMS

ACD	ITL Applied Cybersecurity Division
AI	Artificial Intelligence
AML	Adversarial Machine Learning
ANTD	ITL Advanced Network Technologies Division
ANSI	American National Standards Institute
BGP	Border Gateway Protocol
CAE	Centers of Academic Excellence
CFReDS	Computer Forensic Reference Data Sets
CFTT	Computer Forensic Tool Testing
CIDAR	Cyber Incident Data and Analysis Repository
CMVP	Cryptographic Module Validation Program
CNA	CVE Naming Authorities
COPE	Corporate-owned Personally-Enabled
CPE	Common Platform Enumerations
CPS	Cyber-Physical Systems
CSD	ITL Computer Security Division
CSRC	Computer Security Resource Center
CUI	Controlled, Unclassified information
CVE	Common Vulnerabilities and Exposures
DER	Distributed Energy Resources
DES	Data Encryption Standard
DFARS	Defense Federal Acquisition Regulations Supplement
DHS	Department of Homeland Security
DoD	Department of Defense
DODCAR	DoD Cybersecurity Analysis and Review
EAC	Election Assistance Commission
EL	Engineering Laboratory
EMM	Enterprise Mobility Management
EO	Executive Order
FCSM	Federal Computer Security Program Managers
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GFCE	Global Forum for Cyber Expertise
GSA	General Services Administration
HAVA	Help America Vote Act
HVA	High Value Asset
IAM	Identity and Access Management
ICAM	Identity, Credentials, and Access Management
IAD	ITL Information Access Division
IAPP	International Association of Privacy Professionals
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
IT	Information Technology
ITL	Information Technology Laboratory
ITC	Institute for Testing and Certification
IWG	Interagency Working Group

ITU	International Telecommunication Union
ITU-T	ITU–Telecommunication Standardization Sector
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
LTE	Long Term Evolution
MTD	Mobile Threat Defense
MTI	Mobile Threat Intelligence
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Center of Excellence
NCP	National Checklist Program
NGAC	Next-Generation Access Control
NICE	National Initiative for Cybersecurity Education
NISTIR	NIST Interagency Report
NITRD	Networking and Information Technology Research and Development
NPSBN	National Public Safety Broadband Network
NSRL	National Software Reference Library
NVD	National Vulnerability Database
OIF	Open Identity Federation
OLIR	Online Informative Reference
OMB	Office of Management and Budget
OSCAL	Open Security Controls Assessment Language
PC	Project Committee
P.L.	Public Law
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIV	Personal Identity Verification
PQC	Post Quantum Cryptography
PSCR	Public Safety Communications Research
RDS	Reference Data Set
RFI	Request(s) for Information
RMF	Risk Management Framework
ROV	Route Origin Validation
SCAP	Security Content Automation Protocol
SC	Subcommittee
SCC	Sector Coordinating Councils
SCRM	Supply Chain Risk Management
SDLC	Software Development Life Cycle
SDO	Standards Developing Organizations
SIDR	Secure Inter-Domain Routing
SIM	Subscriber Identity Module
SMB	Small and Medium-Sized Businesses
SSCA	Software and Supply Chain Assurance
SSD	ITL Software and Systems Division
SSDF	Secure Software Development Framework
SSE	Systems Security Engineering
SURF	Summer Undergraduate Research Fellowship
TGDC	Technical Guidelines Development Committee
TLS	Transport Layer Security
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VVSG	Voluntary Voting Systems Guidelines
XML	eXtensible Markup Language
YAML	YAML Ain't Markup Language
ZTA	Zero Trust Architecture

OPPORTUNITIES TO ENGAGE WITH THE NIST CYBERSECURITY PROGRAM DURING FY 2020

NIST provides many opportunities to collaborate and conduct research, including:

- Guest Research Internships opportunities at ITL for 6- to 24-month terms. Qualified individuals should contact ITL (itl_inquiries@nist.gov) to provide qualifications and indicate the area of work that is of interest.
- The NIST Pathways Program offers paths to federal internships for students from high school through post-graduate school as well as careers for recent graduates. It provides training and career development opportunities for individuals who are at the beginning of their federal service. For further details on Pathways and other student programs at NIST, please see https://www.nist.gov/ohrm/staffing/students.cfm.
- The ITL Summer Undergraduate Research Fellowship (SURF) Program is designed to provide hands-on research experience in applied mathematics, statistics, computer security, information access, software testing, and networking technologies. See https://www.nist.gov/itl/how-work-us/itl-surf-program.
- Opportunities for a temporary assignment of government or military personnel for 6- to 24-month details in ITL. Qualified individuals should contact itl_inquiries@nist.gov to provide qualifications and indicate the area of work that is of interest.

- Security Research – NIST occasionally undertakes security work funded by other agencies. Such sponsored work is accepted by NIST when it can cost-effectively further the goals of both NIST and the sponsoring institution.
- More detailed information about ITL's divisions and their research topics are available at https://www.nist.gov/itl/how-work-us/itl-opportunities.

Federal Computer Security Managers' (FCSM) Forum

The FCSM Forum is covered in detail in Focus Area 5 of this report. Membership is free and open to federal employees. For further information, please visit the FCSM Forum website at https://csrc.nist.gov/groups/SMA/forum/membership.html.

Funding Opportunities at NIST

NIST funds industrial and academic research in several ways. The Small Business Innovation Research Program funds R&D proposals from small businesses; see https://www.nist.gov/sbir. 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 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. Funding opportunity information is available at https://www.nist.gov/about-nist/funding-opportunities.

THIS PAGE IS INTENTIONALLY LEFT BLANK