ANNUAL REPORT 2018

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
G2, Incorporated ("G2")
a Huntington Ingalls Company
Annapolis Junction, Maryland

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
https://doi.org/10.6028/NIST.SP.800-206

JANUARY 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

THIS PAGE IS INTENTIONALLY LEFT BLANK

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 800-206
Natl. Inst. Stand. Technol. Spec. Publ. 800-206, 31 pages (January 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-206

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

TRADEMARK INFORMATION

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

FOREWORD

Cybersecurity: Picking up the pace

"*The more things change, the more they stay the same.*" (From a French proverb)

Ten years ago, the National Institute of Standards and Technology (NIST) annual report on cybersecurity featured accomplishments and challenges in quantum computing, encryption, identity management, personal identity verification, vulnerability measurements, assessing the security controls in federal information systems, mobile devices, international standardization, and addressing the needs of small and medium-sized businesses, all of which were among the many pressing topics of the day. Sound familiar?

Reviewing those topics in the NIST Fiscal Year 2008 report on computer security activities and accomplishments might lead some to conclude that the old French proverb is true when it comes to cybersecurity. But in this case, a more appropriate statement might be, "The more things appear to stay the same, the more quickly they actually change."

That certainly is true for the threat environment in which we function today. New attack surfaces, new vulnerabilities, and new attackers emerge constantly. The creativity, the dramatically increased frequency of attacks, and the ready availability of new technologically enhanced modes of attack are even more difficult to identify—much less protect, detect, respond to, and recover from—before they inflict great harm to U.S. organizations and our economy, security, and society in general.

A decade later, these changes have enormous implications in a world that is so much more dependent on digital devices, systems, and connectivity for carrying out both the specialized and ordinary activities that drive our economy and safeguard our security. They create thorny challenges as we seek balance in battling attacks and attackers while preserving our intellectual property, privacy, civil rights, and liberties.

The speed with which our cybersecurity risks change means that everyone involved in managing those risks needs to pick up the pace. That is what NIST is doing with the help of many partners and through varied programs and approaches.

In Fiscal Year 2018, we received and worked on new cybersecurity-related assignments from Congress and the President. Those have led us to focus our attention on assisting small businesses, forging practical solutions to address security concerns raised by the Internet of Things, and updating our guidance on risk management and security controls for federal agencies and others. We also launched major new initiatives, including the development of a voluntary framework for privacy risk management, standards for

post-quantum cryptography, and revisions to Federal Information Processing Standard (FIPS) 140-3,[1] *Security Requirements for Cryptographic Modules*.

One thing has remained constant over the past decade: our commitment to cultivating trust in information and the technology that drives the development and handling of that information. This annual report focuses on some of NIST's most noteworthy cybersecurity achievements in 2018 and offers insights into our current priorities and strategies. For a more complete review of our work, check out our primary cybersecurity website.[2]

NIST welcomes all suggestions for how we can improve our cybersecurity work to better serve the public and private sectors. And, by all means, please join us as we pick up the pace.

Donna F. Dodson
NIST Chief Cybersecurity Advisor

[1] Federal Information Processing Standard (FIPS) 140-3, https://csrc.nist.gov/publications/detail/fips/140/3/final

[2] NIST Cybersecurity, https://www.nist.gov/topics/cybersecurity

TABLE OF CONTENTS

THIS PAGE IS INTENTIONALLY LEFT BLANK

INTRODUCTION

It is often said that cybersecurity is about *people*, *process*, *and technology*. That's a convenient way to think about cybersecurity challenges, and it is the primary approach that the National Institute of Standards and Technology (NIST) takes in carrying out its cybersecurity mission. This report highlights NIST's Fiscal Year (FY) 2018 cybersecurity-related accomplishments and includes many examples of how the NIST Information Technology Laboratory (ITL) delivers value to the nation by focusing on each element of the people, process, and technology triad. Importantly, NIST strives to address those three areas in an integrated fashion, knowing that siloed thinking about cybersecurity is not a viable path to success.

NIST carries out its cybersecurity responsibilities through an open, transparent, and inclusive approach, teaming with organizations in the private sector, non-profit sphere, academia, and government at multiple levels. It does so by cooperating with partners in the United States and abroad who contribute to the research, development, standards, and applications that are all needed to advance both the state-of-the-art and the state-of-practice when it comes to cybersecurity. NIST is also assisted in identifying emerging managerial, technical, administrative, and physical safeguard issues by the Information Security and Privacy Advisory Board (ISPAB).[3] ISPAB is the Federal Advisory Committee[4] that advises NIST, the Secretaries of Commerce and Homeland Security, and the Office of Management and Budget on security and privacy matters.

All of NIST's cybersecurity work is conducted in an environment that demands technical excellence and integrity and that aims to cultivate trust in technologies and institutions. NIST's portfolio of cybersecurity programs works along the full spectrum of cybersecurity challenges and potential, from foundational research to applied engineering and transition to practice.

NIST knows that improving all aspects of cybersecurity is an imperative, not just for the agency but for all of society that relies on technologies, products, and systems. NIST's FY18 premier cybersecurity accomplishments and brief insights into FY19 priorities are captured in the cybersecurity *imperatives* that follow.

[3] Charter of the Information Security and Privacy Advisory Board (ISPAB), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/ispab_charter_2016-2018.pdf

[4] Federal Advisory Committee Act, https://uscode.house.gov/view.xhtml?path=/prelim@title5/title5a/node2&edition=prelim

FROM STATE-OF-THE-ART TO STATE-OF-ACTUAL PRACTICE

NIST's research, standards, guidelines, and recommended best practices are aimed at improving the effectiveness of cybersecurity strategies and measures. They offer an expanding and up-to-date toolkit that information technology (IT) and operational technology (OT) providers and users can put to work to justifiably enhance trust in IT and related technologies. Historically, much of NIST's outputs have been developed primarily for government agencies that are directed by statute and policy to use the Institute's cybersecurity standards and guidelines. However, they also are widely and voluntarily relied upon by private sector cybersecurity practitioners, product vendors and integrators, state and local agencies, and others who see value in NIST's information and services.

NIST recognizes that many systems owners and administrators often find it difficult to sort through the voluminous output of NIST cybersecurity guidance to identify standards and guidelines that apply to their areas of interest. They may struggle to understand how these resources apply to their environments and how NIST's cybersecurity products can be used to address their requirements. They may have difficulty with usability implications of integrating cybersecurity into their systems. These current and potential users need assistance in finding the kind of applications support that NIST offers in addressing some specific cybersecurity implementation problems. In FY18, NIST increased its attention to issues associated with transition to practice with an eye on accelerating adoption of cybersecurity standards, guidelines, and best practices. NIST is ramping up that priority even more steeply in 2019, often through the National Cybersecurity Center of Excellence (NCCoE) as well as throughout the Information Technology Laboratory (ITL). This report spotlights some of those initiatives.

IMPERATIVE 1

Advancing Cybersecurity and Privacy Standards

NIST leverages foundational and applied research as well as extensive experience acquired through decades of leadership and participation in developing national and international standards to advance cybersecurity and privacy standards. Today, these standards activities span cybersecurity, privacy, and cryptography, as well as newer and emerging technology spaces such as Artificial Intelligence and the Internet of Things.

About 40 NIST staff work with industry and other agencies to develop cybersecurity and privacy standards through voluntary consensus Standards Developing Organizations (SDOs). The NIST Cybersecurity Framework (CSF) has provided additional focus and a systematic approach to standards work in this space. This international standards strategy follows the guidelines defined in NISTIR 8074, *Cybersecurity Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*.

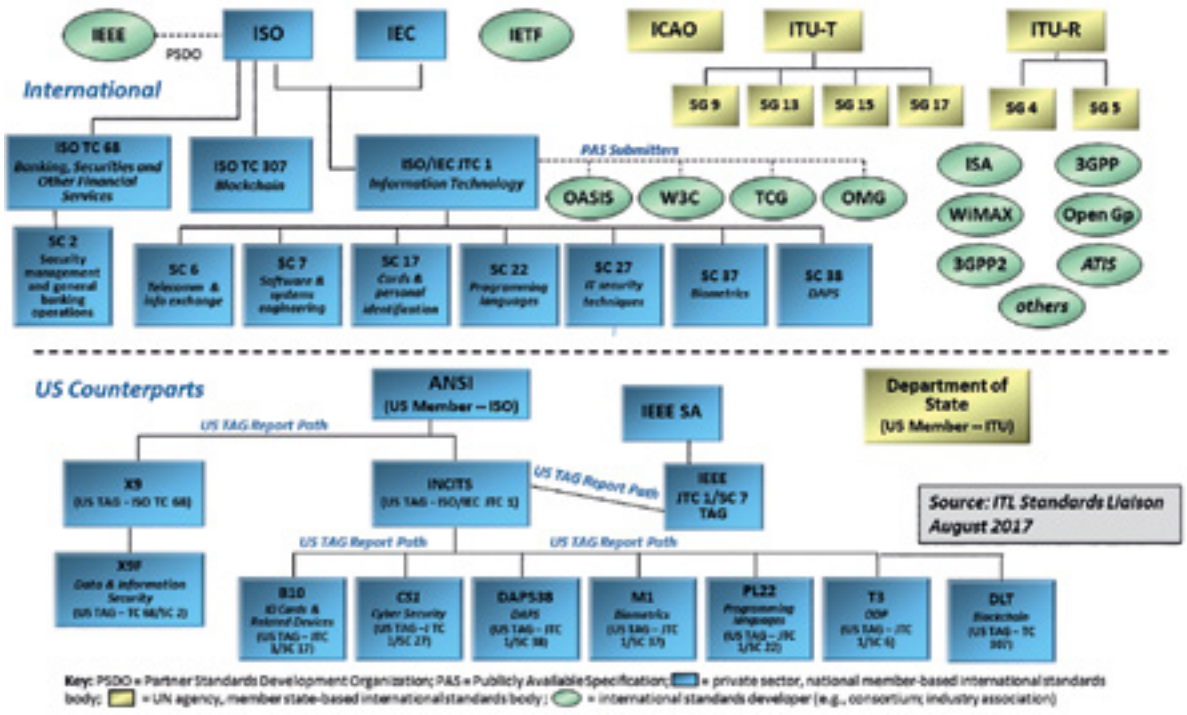

Figure 1. NIST staff participation in cybersecurity standards activities

During FY18, NIST staff actively contributed to and held leadership positions in various SDOs, including the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the T Trusted Computing Group (TCG), the World Wide Web Consortium (W3C), and the 3rd Generation Partnership Project (3GPP). Many of the international SDOs have domestic counterparts. Figure 1, on the previous page; indicates the SDOs in which NIST is actively engaged.

NIST staff have been actively participating in ISO standards bodies to raise awareness and influence the development of privacy standards, including a new family of ISO standards (developed primarily in ISO/IEC Joint Technical Committee (JTC 1)/ Subcommittee (SC) 27) that is aligned with the principles of the NIST Cybersecurity Framework. Notably, NIST staff participates in the Technical Committee ISO/Program Committee (PC) 317 – Consumer Protection: Privacy by Design for Consumer Goods and Services, which focuses on developing ISO 31700 Consumer protection: *Privacy by Design for Consumer Goods and Services*. NIST staff has also been engaged with several privacy standards activities of the ITC 1/SC 27/Working Group (WG) 5. By participating, NIST aims to sustain and promote the development and use of the NIST Privacy Framework and its principles in the international arena.

NIST participation has also grown considerably in Internet of Things (IoT) standardization activities, including JTC 1/SC 41 (IoT architecture and vocabulary, IoT Interoperability, and IoT Applications), JTC 1/SC 27 (IoT aspects of Security and Privacy), IETF – SW Updates for IoT, and the International Telecommunications Union–Telecommunication Standardization Sector (ITU-T): Sector Joint Coordination Activity on IoT and "IoT and Smart Cities." NIST has been instrumental in promoting and participating in the development of a family of voluntary ISO standards that align with NIST's cryptographic module validation standard and related specifications. NIST serves as the project editor for nine of those standards. FIPS 140-3, *Security Requirements for Cryptographic Modules*, points to ISO/IEC 19790, *Security Requirements for Cryptographic Modules*. 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 FY19, NIST staff will continue to lead and participate in cybersecurity and privacy standardization efforts with an increased focus on cybersecurity, privacy, and cryptography, as well as on new and emerging areas such as Artificial Intelligence and the Internet of Things. NIST will continue to provide thoughtful leadership in many SDOs by actively participating in those organizations and contributing publications and papers.

IMPERATIVE 2

Enhancing Risk Management

Increasingly, NIST's work is driven by a recognition that risk management should be a fundamental driver for every organization's decisions about investments in cybersecurity—whether those investments take shape as people, processes, or technology. NIST considers managing risk to be an essential principle and process for organizations of any size or type to employ in planning and carrying out their cybersecurity programs and in making decisions about priorities.

During FY18, NIST made significant strides in producing cybersecurity risk management approaches and tools and assisting organizations in their use. Most notably, these achievements included:

- ***Release of the first update of the Framework for Improving Critical Infrastructure Cybersecurity***, popularly known as simply the "Cybersecurity Framework." First produced in February 2014 with the active involvement of hundreds of organizations in the private and public sectors, Version 1.1 was released in April 2018. Based on the experience of Framework users and changes in the cybersecurity environment and technological advances, the revision added more content related to supply chain risk management and coordinated vulnerability disclosure. NIST added and clarified language regarding cybersecurity measurement with an emphasis on self-assessment. The number of downloads of Version 1.1 has far surpassed that of the initial version.

  Recognizing and seeking to further stimulate international usage of the Cybersecurity Framework, NIST worked on a Spanish language translation, which is now available along with translations or adaptations provided by government agencies and industry leaders in Italian, Japanese, Hebrew, Arabic, and Portuguese. NIST also engaged more purposefully to promote the alignment and use of the Framework, especially in Latin America and Europe. In the international standards arena, NIST vigorously assisted in efforts to include the Framework into a key International Organization for Standardization (ISO) cybersecurity standard, a process that is still under way.

  In addition, NIST included many more resources to aid in using the Cybersecurity Framework, many of which were generated by private sector, non-profit, and government organizations. NIST also launched a series of "Success Stories" highlighting the variety of ways in which organizations of all types and in all sectors are finding value in the Framework. Also in FY18, NIST recognized that new information products and tools are regularly being produced well beyond the initial Informative References included in Version 1.0 and pushed forward with an initiative that establishes a transparent, equitable process for organizations to propose new references, which are intended to be included as online Informative References associated with the Framework.

- ***Update of the NIST Risk Management Framework (RMF)***. For years, the RMF has been a mainstay for federal agencies and others to use in assessing and managing cybersecurity needs and challenges. Two drafts of the new version were produced in FY18—NIST Special Publication (SP) 800-37, Revision 2[5]—before becoming final in early FY19. Updates included significant new guidance in addressing privacy risks and integrating security and privacy into the design of systems. The RMF also references NIST systems security engineering guidance at appropriate points, including NIST SP 800-160,[6] which addresses the engineering of trustworthy secure systems.

  The revised RMF also offers additional guidance on:

  - **Better preparing an organization's senior leaders** to execute the RMF, as well as how to communicate their protection plans and risk management strategies to system implementers and operators.
  - **Incorporating supply chain risk management considerations**. The RMF now addresses growing supply chain concerns, such as counterfeit components, tampering, theft, insertion of malicious software and hardware, poor manufacturing and development practices, and other potentially harmful activities that can impact an organization's systems and systems components.
  - **Supporting security and privacy safeguards**. The RMF update provides organizations with a disciplined and structured process to select controls from the newly developed consolidated security and privacy control catalog in NIST's SP 800-53 Revision 5.[7] This should be valuable to companies and organizations beyond the federal government, considering how high profile the subject of privacy has become as of late.

Importantly, the revised RMF clarifies its relationship to the Cybersecurity Framework. Aligning the RMF with other NIST guidance and publications will help federal agencies which are required to implement multiple frameworks. While adhering to the CSF is voluntary for private companies, its use for the federal government is not optional under Executive Order 13800.[8] Use of the RMF is mandatory for federal agencies in accordance with the Federal Information Security Modernization Act (FISMA[9]). The RMF is also required and in widespread use in the Department of Defense and the intelligence

[5] Special Publication (SP) 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

[6] SP 800-160, Vol. 2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach,* https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/draft

[7] SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations,* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[8] Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[9] Federal Information Security Modernization Act (FISMA), https://www.dhs.gov/fisma

community. That alignment of the Cybersecurity Framework and the RMF is still a work in progress with NIST committed to producing improved guidance in 2019.

- ***Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems***. The FY18 update of this publication addresses 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 as well as the capabilities and services delivered by those systems. It 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 to ensure that those needs are addressed with appropriate fidelity and rigor early on *and* in a sustainable manner throughout the life cycle of the system. NIST also published a draft of the first in a series of specialty publications developed to support the flagship NIST Systems Security Engineering guideline. Volume 2 addresses cyber resiliency considerations for two important yet distinct communities of interest represented by organizations: those conducting new development of IT component products, systems, and services; and those with legacy systems (installed base) currently carrying out day-to-day missions and business functions.
- ***Privacy Framework: An Enterprise Risk Management Tool***. There is growing concern regarding privacy issues across the country and throughout the world. Government organizations are putting into place multiplying privacy requirements that cross borders in their implementation. That is why in FY18, NIST laid the groundwork for developing a risk management-driven approach that could be used by any organization that chooses to do so. The Privacy Framework project, announced in September 2018 and expected to result in a final Framework by late 2019, is being carried out based on the same type and degree of extensive private-public sector collaboration that led to the widely regarded Cybersecurity Framework.

Other risk management-focused NIST cybersecurity accomplishments in FY18 included an update of NIST's recommendations for protecting the confidentiality of controlled, unclassified information (CUI) in non-federal systems and organizations. Safeguarding that CUI is of paramount importance and can directly affect the ability of federal agencies to successfully conduct their assigned missions and business operations. NIST SP 800-171 Revision 1[10] recommends security requirements to those agencies. The FY18 update included editorial changes to select CUI security requirements, additional references and definitions, and an expanded discussion about each CUI requirement.

[10] SP 800-171, Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

IMPERATIVE 3

Strengthening Cryptographic Standards and Validation

Cryptography—the technological foundation for most cybersecurity functions—is constantly under attack by a multiplying array of adversaries that range from individual criminals seeking financial gains to terrorist groups and nation states. If the cryptographic protection for an organization's information technology is defeated or bypassed, the organization—and, potentially, our nation's entire infrastructure system—may be wide open to malicious attack.

NIST is responsible for developing U.S. federal cryptographic standards as well as the technologies and programs used to determine and validate correct implementation of those standards. This has been a mainstay of NIST's computer security work for nearly 50 years. In FY18, NIST continued to work with partners in government, the private sector, and academia in the United States and around the globe to confront a variety of urgent technical and implementation challenges to cryptographic security. These included:

- ***Post-Quantum Cryptography***. 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. If large-scale quantum computers are ever built, they will be able to break many of the public key cryptosystems currently in use, seriously compromising the confidentiality and integrity of digital data. During FY18, NIST continued to prioritize work on *post-quantum cryptography* (also called quantum-resistant cryptography) with the ambitious goal of developing cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

  After an earlier call to the public to submit post-quantum algorithms[11] that could resist a quantum computer's onslaught, from FY18 to FY19 NIST worked with the larger cryptography community to narrow the field from 69 submitted algorithms to 26. The remaining algorithms are those which NIST mathematicians and computer scientists consider to be the strongest candidates. Next, NIST is asking the cryptography community to focus on analyzing how these algorithms will perform in the real world (e.g., how they will fit into the internet protocols currently in use). This second round of analysis focuses more heavily on evaluating the submissions' performance across a wide variety of systems, not just in big computers and smartphones.

[11] NIST Asks Public to Help Future-Proof Electronic Information, https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information

- ***Lightweight Cryptography***. Many different devices and systems—including smart cards, tiny devices for IoT use, and individual microchips—need effective encryption yet have limited processor power. These devices and systems are vital in sensor networks, healthcare, distributed control systems, and cyber physical systems. Because the majority of current cryptographic algorithms were designed for desktop/server environments, many do not fit into constrained devices. Quantum-resistant algorithms that can perform this sort of "lightweight cryptography" are sorely needed. In FY18, NIST invited submissions of candidate lightweight cryptographic algorithms[12] that provide adequate security for environments in which processing performance is constrained and where the performance of current NIST cryptographic standards is not acceptable. In FY19, NIST aims to pare down those candidates for further evaluation and public review.
- ***Responding to and Anticipating Other Technology Developments***. Recent developments in cryptographic technologies, including the use of blockchain techniques, have driven the need for updated cryptographic key establishment and implementation guidance. In FY18, NIST released multiple documents designed to fulfill those needs. Significant accomplishments included:
    - Release of random number generation guidelines[13] and an online public source[14] of random numbers
    - Updated recommendations for best practices for key management organization
    - Additional guidance on transitioning[15] to more effective cryptography
    - Advanced automated testing and validation [16] of the correctness of algorithms (see Text Box #3), including introduction of a new protocol to the international standards development process

In FY19, NIST will begin revising additional guidance, convene[17] a stakeholder workshop on threshold cryptography, complete development[18] of a hardware chip that implements improved techniques, and continue to work with external collaborators on developing consensus-based blockchain standards.

[12] Lightweight Cryptography Project, https://csrc.nist.gov/projects/lightweight-cryptography

[13] SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation,* https://csrc.nist.gov/news/2018/nist-announces-the-release-of-sp-800-90b

[14] NIST Randomness Beacon, Version 2.0 Beta, https://beacon.nist.gov/home

[15] SP 800-131A, Rev. 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/archive/2018-07-19

[16] Automated Cryptographic Validation (ACV) Testing, https://csrc.nist.gov/publications/detail/itl-bulletin/2018/09/automated-cryptographic-validation-testing/final

[17] Threshold Cryptography, https://csrc.nist.gov/projects/threshold-cryptography

[18] Circuit Complexity, https://csrc.nist.gov/projects/circuit-complexity

CRYPTO STANDARD = HUGE $$ IMPACT

In FY18, NIST released a study[19] that estimated a $250 billion economic impact from the development of its Advanced Encryption Standard (AES) from 1996-2017. AES is a cryptographic algorithm[20] to encrypt and decrypt electronic information. It was approved for use by the Federal Government in November 2001 and has since been widely adopted by private industry. Today, AES protects everything from classified data and bank transactions to online shopping and social media apps. According to the study, NIST's investment in AES has been repaid many times over—the study's most conservative estimate shows a 29 to 1 benefit-to-cost ratio for the AES program. The estimated benefit-to-cost ratio for the whole economy was 1,976 to 1. The report relied on a survey of government and private sector consumers of encryption systems and private integrators who develop and produce encryption hardware or software.

In 1997, NIST launched its effort to identify a new standard encryption algorithm for the Federal Government after recognizing that the Data Encryption Standard (DES), adopted 20 years earlier, was growing vulnerable in the face of advances in cryptanalysis and the exponential growth in computing power. In October 2000, following a three year, open international competition, NIST announced its proposal for the replacement standard: an algorithm submitted by two cryptographers from Belgium. The unclassified, publicly disclosed encryption algorithm is available royalty-free and is used by the U.S. Federal Government in its Federal Information Processing Standard (FIPS) and voluntarily by private organizations worldwide.

[19] The Economic Impact of the Advanced Encryption Standard, 1996-2017, https://csrc.nist.gov/publications/detail/white-paper/2018/09/07/economic-impacts-of-the-advanced-encryption-standard-1996-2017/final

[20] FIPS 197, https://csrc.nist.gov/publications/detail/fips/197/final

AUTOMATING CRYPTOGRAPHIC TESTING

Several years ago, NIST launched a project to automate much of the testing required under its cryptographic validation programs. Automated cryptographic algorithm testing was completed in 2018, and NIST is now developing methods to automate the testing of cryptographic modules. These efforts in automation are intended to provide a higher trust in the assurance claims made by the product developers in an efficient and cost-effective manner that allows the vendors' conformance efforts to keep pace with the changing IT landscape. By investing in a more robust testing infrastructure, NIST anticipates that product vendors will take advantage of this service by validating their products more often, which will produce more secure products. In FY19, NIST will put more responsibility for generating evidence of conformance in the hands of industry by leveraging automated test processes that will reduce time to market, slice costs to maintain compliance, and ensure that the Federal Government has effective and up-to-date technologies.

IMPERATIVE 4

Advancing Cybersecurity Research and Applications Development

Beyond cryptography-related priorities, 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 organizations' mission-critical information systems. Accomplishments included:

- ***Cloud Computing Security and Forensics***. During FY18, NIST continued to develop publications, promote national and international standards and specifications, and demonstrate how to meet those standards and specifications to support the effective and secure use of cloud computing.[21] NIST collaborated with industry[22] to implement the Cloud Security Architecture Tool (CSAT),[23] leveraging the NIST Cybersecurity Framework to architect a cloud-based information system and identify necessary security controls. Aiding transition to practice, NIST collaborated with industry to initiate a cloud security project to show one way to increase security and privacy for cloud workloads on hybrid cloud platforms. Based on public comments, NIST also updated a guide that shows how to reduce opportunities for bad actors to attack enterprises via the cellular and WiFi connections on mobile devices; final publication is planned for FY19.[24] In addition, the Cloud Forensic Science Working Group continued to define a cloud forensics reference architecture. Continuation of a trusted cloud capability demonstration, CSAT, and forensics activities are planned for FY19.

- ***Low Power Wide Area Networks***. Diverse applications of Internet of Things and Cyber-physical Systems (IoT/CPS) require various network technologies be optimized for specific use cases. A low-power wide-area network (LPWAN) is a set of telecommunication specifications and protocols that satisfy both low power consumption (i.e., network of inexpensive sensors) and wide area coverage (i.e., smart city deployments). In order to build an understanding of the security and trust issues of LPWAN-based telecommunications, NIST prototyped two use cases for LPWAN-based sensor networks in FY18. The use case prototypes included a remote access adapter for a NIST climate monitoring station and a real-time tracking system for the NIST Campus Shuttle that was

[21] NIST Cloud Computing Program (NCCP), https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

[22] SBIR Success Story: InfoBeyond Technology LLC, https://www.nist.gov/tpo/sbir-success-story-infobeyond-technology-llc

[23] NIST Cloud Security Architecture Tool (CSAT), https://www.fbcinc.com/e/fitsc/presentations/Iorga-fitsc-csat_with_rmfoscal.pdf

[24] SP 1800-4, *Mobile Device Security: Cloud and Hybrid Builds*, https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/cloud-hybrid

able to receive sensor data from devices located 5 miles away from the receptor. Potential security weaknesses and possible mitigations arising out of this experience with LPWAN technology are now being investigated. Researchers have learned that WiFi and Bluetooth do not naturally apply to some IoT/CPS deployment scenarios, particularly when deployment is outside, requires battery operation for extended periods, or must operate over a long range. In FY18, the team also deployed an LPWAN Infrastructure that was integrated with NIST's internal network, NIST-Net, satisfying all security policies required by NIST. In FY19, the NIST Engineering Laboratory (EL), NIST/ITL, and National Institute of Metrology, Standardization and Industrial Quality (INMETRO) team will study the implementation of LPWAN on the Smart Grid and investigate LPWAN in the context of Smart Grid cybersecurity guidelines.

- ***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 developing OSCAL—a standard for representing different categories of information about the publication, implementation, and assessment of security controls. In FY18, NIST completed a control catalog and profile schemas and began developing an implementation schema for representing system security plans (SSP) in OSCAL. The team validated the approach with several use cases. In FY19, NIST will continue to develop other approaches involving the Cybersecurity Framework as well as assessments and assessment results.

- ***Combating Ransomware***. NIST has placed a high priority on identifying and demonstrating tools for identifying, protecting against, detecting, responding to, and recovering from ransomware attacks and other events that are destructive to systems and operations. In FY18, NIST released *Data Integrity: Recovering from Ransomware and Other Destructive Events* (SP 1800-11)[25] for public comment and initiated two other ransomware projects, *Data Integrity: Identifying and Protecting Against Ransomware and Other Destructive Events*[26] and *Detecting and Responding to Ransomware and Other Destructive Events*.[27] Finalization of SP 1800-11 and development of practice guides for the identification and protection and the detection and response projects are planned for FY 2019.

[25] SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover

[26] *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect

[27] *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events,* https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond

- ***Roots of Trust***. Modern computing devices consist of varied hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are rooted in software that, along with all underlying components, must be trusted and not tampered with. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon them. Achieving stronger security assurances may be possible by grounding security mechanisms in highly reliable and secure hardware, firmware, and software components that perform specific, critical security functions. In FY18, NIST built on earlier work focused on protecting boot firmware to develop new technical guidelines and recommendations for supporting the resiliency of platform firmware and data against potentially destructive attacks. *Platform Resiliency Guidelines* (SP 800-193)[28] promotes resiliency in platforms by describing security mechanisms for protecting against unauthorized changes, detecting unauthorized changes that occur, and securely recovering from attacks. In FY19, NIST plans to continue outreach to stakeholders to encourage the development of more secure and reliable systems and investigate how roots of trust can support other security needs, including supply chain assurance.

[28] SP 800-193, *Platform Firmware Resiliency Guidelines,* https://csrc.nist.gov/publications/detail/sp/800-193/final

IMPERATIVE 5

Improving Cybersecurity Awareness, Training, 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 users' and providers' 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.

In FY18, NIST placed a greater emphasis on improving the public availability of information resources by providing them to small businesses in the form of briefings, advancing awareness and understanding of human factors contributing to cybersecurity challenges, and recommendations for steps to address workforce shortage and training issues.

FY18 web-accessible information resources included: the Computer Security Resource Center (CSRC),[29] National Software Reference Library (NSRL),[30] Security Automation Reference Data and the National Vulnerability Database (NVD),[31] National Checklist Program (NCP) repository,[32] Software Assurance and Quality Software Assurance Reference Dataset (SARD),[33] and Computer Forensics Tool Testing Project tool catalog[34] and reference data sets.[35] Ongoing federal outreach efforts include the Software and Supply Chain Assurance (SSCA) Forum,[36] the Federal Computer Security Managers' (FCSM) Forum,[37] and the Federal Information Systems Security Educators' Association (FISSEA).[38]

- ***Cybersecurity for Small Businesses***. Small and medium-sized businesses (SMBs) represent approximately 95 % of all businesses and are often considered to be the backbone of the U.S. economy. 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,

[29] Computer Security Resource Center (CSRC), https://csrc.nist.gov

[30] National Software Reference Library (NSRL), https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl

[31] National Vulnerability Database (NVD), https://nvd.nist.gov/

[32] National Checklist Program (NCP) Repository, https://nvd.nist.gov/ncp/repository

[33] NIST Software Assurance Reference Dataset (SARD) Project, https://samate.nist.gov/sard/

[34] Computer Forensics Tools and Techniques Catalog, https://toolcatalog.nist.gov/

[35] Computer Forensic Reference Data Sets (CFReDS), https://www.cfreds.nist.gov/

[36] Software and Supply Chain Assurance (SSCA) Forum, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/ssca

[37] Federal Computer Security Managers' Forum, https://csrc.nist.gov/events/2018/federal-computer-security-managers-forum-2-day

[38] Federal Information Security Educators (FISSEA), https://csrc.nist.gov/projects/fissea

together with interagency and industry partners and collaborators. The NIST Small Business Cybersecurity Act, which became law on August 14, 2018, 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." During FY18, the NIST Small Business Outreach Program began updating the Small Business Cybersecurity Corner website to make resources easier to find and use. In FY19, those training materials and accompanying resources will be expanded based on contributed cybersecurity resources and feedback received from federal partners and the public.

- ***National Initiative for Cybersecurity Education (NICE)***. Hosted by NIST, NICE seeks to help equip, promote, and energize a robust network of organizations that address cybersecurity education, training, and workforce development. 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*.[39]

Figure 2: The Seven Categories of the NICE Framework

In FY18, fulfilling a directive in Executive Order 13800,[40] NICE joined with the Department of Homeland Security to prepare a report to the President[41] that made a series of recommendations. In their transmittal to the President, the Commerce and Homeland Security Secretaries noted that "in both the private and public sectors, cybersecurity practitioners and educators are vital to our national security—especially since other nations are paying greater attention to their cybersecurity workforce needs and the cybersecurity weaknesses of their adversaries." The report was based on an analysis of available data and the information and views shared by businesses, educational organizations, training and certification providers, government agencies at multiple levels, and individuals. Findings and specific, forward-thinking, and actionable

[39] NICE Cybersecurity Workforce Framework, https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[40] Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[41] *A Report to the President: Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future,* https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/supporting-growth-and-sustainment-of-the-cybersecurity-workforce/final

recommendations addressed both public and private sector needs (see Text Box #4). In FY19, the President issued another executive order[42] directing agencies to implement those recommendations

CYBERSECURITY WORKFORCE RECOMMENDATIONS TO THE PRESIDENT

- The Nation should set an ambitious vision and action plan-of-attack to "prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity."
- The Federal Government should lead in launching a high-profile national *Call to Action* to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
- The Administration should focus on and recommend long-term authorization and sufficient appropriations for high-quality, effective cybersecurity education and workforce development programs in its budget proposals in order to grow and sustain the cybersecurity workforce.
- Federal departments and agencies must move quickly to address major needs relating to recruiting, developing, and retaining cybersecurity employees and continue to implement the Federal Cybersecurity Workforce Strategy[43] and the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA).[44]
- The private and public sectors need to transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.
- The private and public sectors need to align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers.
- The private and public sectors need to establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

In FY18, the NICE program worked to enhance CyberSeek.[45] This tool was developed in partnership with industry to help employers, job seekers, policy makers, training providers and guidance counselors find information on the supply

[42] *Executive Order on America's Cybersecurity Workforce*, https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

[43] Federal Cybersecurity Workforce Strategy, https://chcoc.gov/content/federal-cybersecurity-workforce-strategy

[44] Federal Cybersecurity Workforce Assessment Act, https://www.congress.gov/bill/114th-congress/senate-bill/2007

[45] CyberSeek, https://www.nist.gov/itl/applied-cybersecurity/nice/cyberseek

of workers with relevant credentials and to show career pathways in cybersecurity that map opportunities for advancement in the field.

- ***Usability and Cybersecurity***. Too often, sound cybersecurity components and practices are not employed because of user resistance. In FY18, NIST advanced research that examined usability attributes and reasons for user resistance. The topics addressed included phishing, password policies, usable privacy, cryptographic development, and youth password perceptions and behaviors. FY18 marked the beginning of a multi-year research effort to examine youth security practices, behaviors, and perceptions with the goal of developing useful guidance to help youth learn, understand, and ultimately practice good cybersecurity behaviors. In FY18, a paper documenting the results of the first school district surveyed (Ohio)—which included students in grades 3 to 8—was completed. Further analysis of all five school systems' survey data is being conducted in FY19 and will include descriptive statistics and a follow-up survey that examines parents' password practices and their involvement (or lack of involvement) with the password usage of their grade school children.

RESULTS OF ONLINE SURVEYS OF CRYPTOGRAPHIC DEVELOPERS

During FY18, the Usability and Cybersecurity team published a paper reporting the results of online surveys of organizations involved in cryptographic development. Findings revealed that organizations used cryptography for a wide range of purposes. Most relied on generally accepted, standards-based implementations as guides while others developed their own implementations by drawing from non-standards resources. The results highlighted the challenges for organizations that undertake cryptographic development, including difficulties in recruiting and managing talent, disruptions to the product lifecycle, and trouble explaining the security value of products to customers. Interviews of representatives from organizations that include cryptography in their products suggested a strong security mindset demonstrated by robust organizational security culture and the deep expertise of those performing cryptographic development. The results encourage additional research initiatives to explore variations in those implementing cryptography, which can aid in transferring lessons learned from more security-mature organizations to the broader development community through educational opportunities, tools, and other mechanisms.

IMPERATIVE 6

Enhancing Identity and Access Management

Properly managing access to IT systems, processes, and information is central to managing cybersecurity risks and a priority for NIST's cybersecurity program. NIST engages and collaborates with standards bodies and consortia such as the International Organization for Standardization (ISO),[46] the Internet Engineering Task Force (IETF),[47] the Fast IDentity Online (FIDO) Alliance,[48] the Open Identity Federation (OIF), and the Kantara Initiative.[49]

MOVING AWAY FROM PASSWORDS

In response to a widely recognized need, NIST continued to advance the challenge of moving away from passwords and plans to publish a key report in 2019 with its latest research findings and recommendations. In 2018, NIST:

- Continued to investigate Authentication for Law Enforcement Vehicle Systems[50] project requirements and
- Revised high visibility publications, including: the *Attribute Based Access Control* (SP 1800-3)[51] guide that shows how to manage access to networked resources more securely and efficiently; the *Mobile Application Single Sign-on: Improving Authentication for Public Safety and First Responders* (SP 1800-13)[52] guide that shows how single sign-on can be used efficiently and securely on mobile devices to access restricted information; and the *Multifactor Authentication for E-Commerce* (SP 1800-17)[53] guide that shows how organizations can efficiently implement multi-factor authentication in a user-friendly manner to protect customers' information from being used for fraudulent purchases.

In FY19, NIST intends to finalize SP 1800-3, SP 1800-13, and SP 1800-17 based on comments from industry and the public.

---

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

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

[48] Fast IDentity Online Alliance (FIDO), https://fidoalliance.org/

[49] Kantara Initiative, https://kantarainitiative.org/

[50] Authentication for Law Enforcement Vehicle Systems, https://www.nccoe.nist.gov/projects/project-concepts/authentication-law-enforcement-vehicle-systems

[51] SP 1800-3, *Attribute Based Access Control,* https://www.nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

[52] SP 1800-13, *Mobile Application Single Sign-On*, https://www.nccoe.nist.gov/projects/use-cases/mobile-sso

[53] SP 1800-17, *Multifactor Authentication for E-Commerce*, https://www.nccoe.nist.gov/projects/use-cases/multifactor-authentication-ecommerce

- ***Personal Identity Verification (PIV)***.[54] As charged by Homeland Security Presidential Directive-12, NIST developed and maintains the Federal Information Processing Standard (FIPS) for personal identity verification (PIV) of federal employees and contractors (FIPS 201).[55] In FY18, the agency revised its guideline for the use of PIV credentials for physical access (SP 800-116)[56] and sought comments on a draft report demonstrating how commercial technologies can be used to issue and use PIV credentials on mobile devices. NIST also requested public comments SP 1800-12,[57] a guide that shows how to leverage identity-proofing and vetting results of current and valid PIV credentials to enable two-factor authentication to information technology systems via mobile devices. In FY19, NIST plans to revise FIPS 201 to reflect technology changes and evolving practices regarding authentication using PIV credentials.

- ***Policy Machine – Next Generation Access Control***. NIST is developing an Attribute-Based Access Control (ABAC) framework called the "Policy Machine," which is designed to align with a Next Generation Access Control emerging standard from the American National Standards Institute/ International Committee for Information Technology Standards (ANSI/ INCITS). In FY18, NIST updated its Policy Machine Web Services through GitHub as an open-source distribution to support widespread experimentation of web-based applications.

- ***Access Control and Privilege Management***. NIST continued to provide improved guidance for dealing with access control and privilege management issues. This included publishing an *Attribute-Based Access Control* textbook; researching a general access control mechanism for cloud computing services; enhancing conformance verification for access control policies; revising SP 1800-9[58]—a guide that shows how to manage disparate identity and access mechanisms and systems as a comprehensive identity and access management system; and developing SP 1800-18[59]—a guide that shows a way to detect and protect against IT user accounts that have administrative or "super user" privileges being misused. In FY19, NIST plans to finalize SP 1800-9 and continue its work with private sector communities of interest to align its guidance and capability demonstrations with the needs of industry and private citizens.

---

[54] Personal Identity Verification of Federal Employees and Contractors, https://csrc.nist.gov/projects/piv

[55] FIPS 201-2, https://csrc.nist.gov/publications/detail/fips/201/2/final

[56] SP 800-116, Rev. 1, *Guidelines for the Use of PIV Credentials in Facility Access*, https://csrc.nist.gov/publications/detail/sp/800-116/rev-1/final

[57] SP 1800-12, *Derived PIV Credentials Practice Guide,* https://www.nccoe.nist.gov/library/derived-piv-credentials-nist-sp-1800-12-practice-guide

[58] SP 1800-9, *Access Rights Management for Financial Services Sector*, https://www.nccoe.nist.gov/projects/use-cases/access-rights-management

[59] SP 1800-18, *Privileged Account Management for Financial Services Sector,* https://www.nccoe.nist.gov/projects/use-cases/privileged-account-management

IMPERATIVE 7

Bolstering Infrastructure Protection

NIST is focusing on three major national critical infrastructure programs where effective cybersecurity is a vital element: the internet infrastructure, Energy Infrastructure Cybersecurity, and cybersecurity aspects of electronic voting.

- ***Internet Infrastructure Protection (IIP)***. NIST works with industry to develop the measurement science, new standards, and standards implementation capabilities necessary to ensure the resilience and security of the global Internet. In FY18, research focused on developing measurement and modeling techniques necessary to understand, predict, and control the behavior of internet-scale networked information systems, especially foundational routing and communications protocols. This includes the internet's Domain Name System (DNS), Border Gateway Protocol (BGP), and electronic mail and messaging infrastructures. In addition, NIST has been giving special attention to systemic vulnerabilities in core internet technologies such as those that enable distributed denial-of-service (DDoS) attacks on a massive scale.

  In FY18, multiple NIST publications contributed to showing how to remedy serious security and robustness vulnerabilities in network infrastructures. Cybersecurity practice guides were developed with step-by-step example solutions using commercially available technologies. These included SP 1800-6,[60] which shows how to combat spear phishing by improving assurance of the correctness of email sources, destinations, and cryptographic protection of email, and SP 1800-14,[61] which explains how service providers can better control routing of internet traffic. NIST also initiated a network infrastructure project to illustrate how to better manage cryptographic certificates in order to reduce system outage and security breach risks (SP 1800-16).[62] In addition to completing ongoing network security activities in FY19, NIST plans to collaborate with government and private industry on a major feasibility demonstration effort for transitioning systems and services from IPv4 to improved IPv6 information transfer protocols.

[60] SP 1800-6, *Domain Name System-Based Electronic Mail Security*, https://www.nccoe.nist.gov/projects/building-blocks/secured-email

[61] SP 1800-14, *Protecting the Integrity of Internet Routing Practice Guide*, https://www.nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing

[62] SP 1800-16, *Securing Web Transactions Practice Guide*, https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management

DOMAIN NAME SYSTEM-BASED ELECTRONIC MAIL SECURITY

NIST's Special Publication 1800-6, *Domain Name System-Based Electronic Mail Security,* was published in January 2018. This publication documents the use of products that improve security and integrity for electronic mail users by employing the DNS-based Authentication of Named Entities (DANE) protocol to authenticate domain addresses (e.g., @nist.gov) for electronic mail and STARTTLS protocol, which provides a way to take an existing insecure connection and upgrade it to a secure connection using secure transmission protocols. Since its publication, there has been a sharp increase in the number of internet domains that deploy DANE (608 % from February 2018 to February 2019). Moreover, the Department of Homeland Security's Binding Operational Directive 18-01 now provides compulsory direction to federal executive branch departments and agencies to employ email authentication and specifies that all internet-facing email servers offer the STARTTLS protocol.

- ***Energy Infrastructure Cybersecurity***. Under the Energy Independence and Security Act (EISA),[63] NIST has a leading role in collaborating with the private sector to coordinate and accelerate smart grid[64] interoperability and security standards. Multiple NIST laboratories are involved in this effort to advance measurement science, leading to better utilization of assets, improved grid reliability, and greater use of renewable energy sources in the grid. This is accomplished through a combination of research, standardization, testing and implementation of the NIST Smart Grid Interoperability Framework.[65] In FY18, NIST:
  - Conducted a grid edge experiment to understand the performance impact of cybersecurity capabilities on resource-constrained components of the grid;
  - Published SP 1800-2,[66] a guide that shows how organizations can more securely and effectively manage access to networked operational technology (OT) devices and systems on which their operations depend; and
  - Revised SP 1800-7,[67] Smart Grid Cybersecurity Committee, a guide that explains how energy companies can capture, transmit, analyze, and store real-time or near real-time data for their systems to detect, analyze, and remediate anomalous conditions.

[63] Energy Independence and Security Act of 2007, https://www.congress.gov/bill/110th-congress/house-bill/6

[64] SmartGrid, https://www.smartgrid.gov/

[65] Smart Grid Framework, https://www.nist.gov/engineering-laboratory/smart-grid/smart-grid-framework

[66] SP 1800-2, *Identity and Access Management (IdAM)*, https://www.nccoe.nist.gov/projects/use-cases/idam

[67] SP 1800-7, *Situational Awareness for Electric Utilities*, https://www.nccoe.nist.gov/projects/use-cases/situational-awareness

NIST also began to incorporate cybersecurity risk management into the next version of the Smart Grid Interoperability Framework. In FY19, NIST will continue to develop the next version of the Smart Grid Interoperability Framework 2.0, chair the Smart Electric Power Alliance (SEPA)[68] Smart Grid Cybersecurity Committee, support the Department of Energy's Cyber Resilient Energy Delivery Consortium (CREDC) program,[69] finalize SP 1800-7,[70] and undertake capability demonstration and documentation activities for an Energy Sector Asset Management[71] project.

SECURITY ASPECTS OF ELECTRONIC VOTING

The Help America Vote Act (HAVA)[72] encouraged upgrading voting equipment across the United States and established the Election Assistance Commission (EAC)[73] and the Technical Guidelines Development Committee (TGDC).[74] NIST chairs the TGDC and provides technical support related to human factors, security, and laboratory accreditation. Most significantly, in FY18, the TGDC adopted a new version of the Voluntary Voting Systems Guidelines (VVSG)[75] and principles developed by NIST and the EAC. In FY19, NIST will continue leading the public working groups to inform the development of voting system requirements and test strategies based on the principles and guidelines. Additionally, NIST will support the development of a Cybersecurity Framework Profile to help better manage cybersecurity risk in the election infrastructure.

[68] Smart Electric Power Alliance (SEPA), https://sepapower.org/

[69] Cyber Resilient Energy Delivery Consortium (CREDC), https://cred-c.org/

[70] SP 1800-7, *Situational Awareness for Electric Utilities*, https://www.nccoe.nist.gov/projects/use-cases/situational-awareness

[71] SP 1800-23, *Energy Sector Asset Management Practice Guide*, https://www.nccoe.nist.gov/projects/use-cases/energy-sector/asset-management

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

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

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

[75] Voluntary Voting System Guidelines, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

IMPERATIVE 8

Securing Emerging Technologies

Information technology is always rapidly evolving. The extraordinary growth of smart, connected technologies is a particularly promising and concerning arena since any small, connected element is a potential point of vulnerability to the local system and all connected systems. Recent attacks on major network providers have included sustained cyber-attacks launched through fringe (but connected) parts of the system. These have included WiFi controllers, closed circuit television (CCTV) cameras, printers, and baby monitors. NIST focused significant attention in FY18 on emerging network security topics, such as cybersecurity for the Internet of Things (IoT), low-power wide-area networks, public safety broadband networks, fog computing, and quantum computing. In FY19, more effort will shift to cybersecurity issues associated with the potential for 5G networks on security requirements of new use cases and new network architectures as well as the impact of artificial intelligence and machine learning on cyber defenses.

- ***Cybersecurity for IoT***. In FY18, to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their IoT devices, NIST published NISTIR 8228[76] for review and comment by industry and the public. Also in FY18, NIST initiated an Identity and Access Management for Smart Home Devices[77] project and a feasibility demonstration project mapped to NISTIR 8228 that shows how to use existing security protocols to reduce opportunities for malicious access to IoT devices from the internet. That set the stage for publishing the resulting practice guide, SP 1800-15,[78] in FY19 for review and comment by industry and the public. The guide is being expanded to include improved support for small business environments, control of access to and by IoT devices that do not yet support the Manufacturer Usage Description (MUD) protocol, and access to and utilization of threat signaling capabilities. NIST also co-chairs the IoT Task Group of the Interagency International Cybersecurity Standardization Working Group (IICS WG) with the Department of Homeland Security (DHS). In addition, NIST is actively engaging public and private sector stakeholders to better understand the IoT threat landscape and challenges (see the draft of NISTIR 8200).[79] In FY19, after considering public comments, NIST plans to publish final versions of those documents and continue collaborating with stakeholders in developing guidance for IoT security and privacy.

[76] NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, https://csrc.nist.gov/publications/detail/nistir/8228/final

[77] Identity and Access Management for Smart Home Devices, https://www.nccoe.nist.gov/projects/project-concepts/idam-smart-home-devices

[78] SP 1800-15, *Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*, https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

[79] NISTIR 8200, *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, https://csrc.nist.gov/publications/detail/nistir/8200/archive/2018-02-14

Figure 3: IoT for the GSA Smart Building, from NISTIR 8200

BOTNET REPORT

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats,[80] released on May 30, 2018, outlines government and the private sector actions that would reduce the threat of botnets and similar cyberattacks. It responds to the May 11, 2017, *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[81] That order directed the Secretaries of Commerce and Homeland Security to lead "an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." In the course of the year-long effort launched by the Executive Order, the Departments determined that the opportunities and challenges of working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes:

1. Automated, distributed attacks are a global problem.
2. Effective tools exist but are not widely used.
3. Products should be secured during all stages of the lifecycle.
4. Awareness and education are needed.
5. Market incentives should be more effectively aligned.
6. Automated, distributed attacks are an ecosystem-wide challenge

Five complementary and mutually supportive goals were identified that, if realized, would dramatically reduce the threat of automated, distributed attacks and improve the resilience and redundancy of the ecosystem:

Goal 1: Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace.

Goal 2: Promote innovation in the infrastructure for dynamic adaptation to evolving threats.

Goal 3: Promote innovation at the edge of the network to prevent, detect, and mitigate automated, distributed attacks.

Goal 4: Promote and support coalitions between the security, infrastructure, and operational technology communities domestically and around the world.

Goal 5: Increase awareness and education across the ecosystem.

[80] *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final

[81] Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, https://csrc.nist.gov/topics/laws-and-regulations/executive-documents/eo-13800

- ***National Public Safety Broadband Network (NPSBN)***. Federal statute directs NIST to conduct research and development that supports 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. In FY18, supported by the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR)[82] program, NIST expanded its support to provision mobile application vetting tools for public safety mobile application security and continued its research into identity management, data and application isolation technologies, wearable devices, and broadband standards. In FY19, NIST will continue to strengthen its relationship with public safety and commercial telecommunications stakeholders. Work concerning mobile application vetting and cybersecurity will continue to evolve as NIST refines methods for evaluating tools as well as the test cases used in those evaluations. The PSCR program also plans fund grants and prize challenges to solve current problems and fill future gaps in public safety broadband technology.
- ***Fog Computing***. New concepts and technologies are needed to manage a growing fleet of IoT devices to ensure minimal latency (delay) across a distributed and decentralized model. Fog computing is the next new technology that offers a distributed and federated compute model, which provides low-latency computational resources, elastic capabilities, and data analytics and management. In 2018, NIST facilitated an effort to document the fog computing conceptual model to help foster productive conversations among practitioners and researchers and to guide the advancement of technologies that support this model. The publication[83] also introduces fog computing's subsidiary concept, mist computing, and identifies these concepts in relation to cloud computing, cloudlets, and edge computing.

[82] Public Safety Communications Research Division (PSCR), https://www.nist.gov/ctl/pscr

[83] SP 500-325, *Fog Computing Conceptual Model*, https://csrc.nist.gov/publications/detail/sp/500-325/final

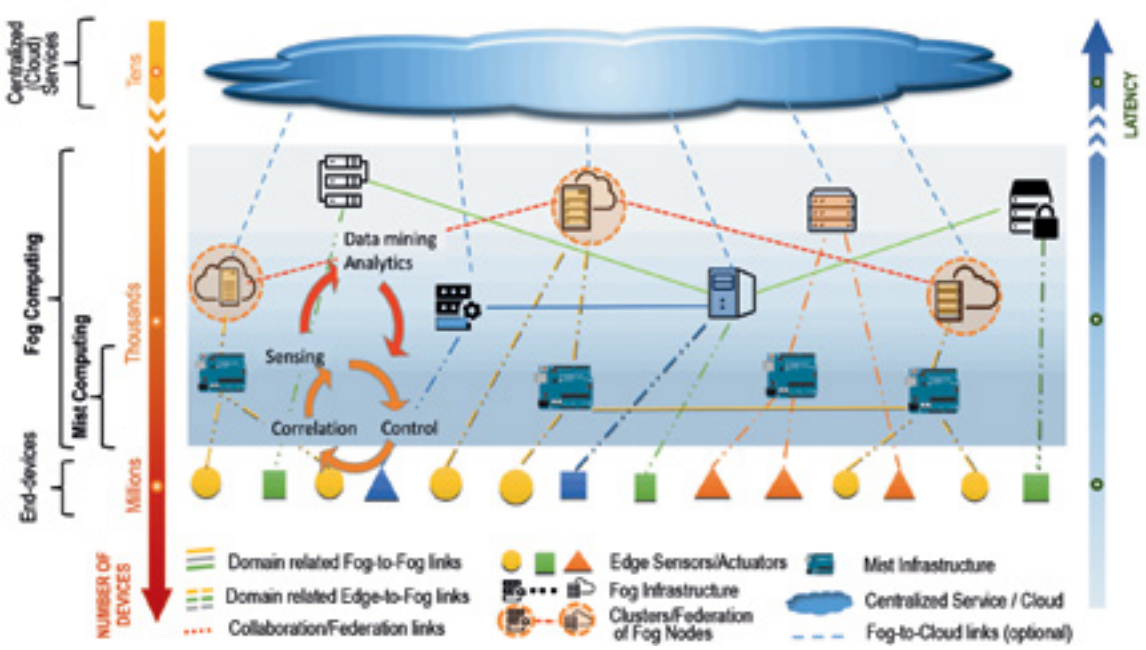

Figure 4: Fog computing supporting a cloud-based ecosystem for smart end-devices

IMPERATIVE 9

Advancing Security Test and Measurement Tools

Widespread adoption and continuing support for cybersecurity requires:

- Testing and documentation of the effectiveness of recommended technologies and practices,
- Means for measuring the effectiveness of recommended technologies and practices,
- Monitoring and collection of information regarding asset inventories and security status, and
- Effective presentation of the results to those who have responsibility for allocating resources within organizations.

NIST is approaching the challenge of security status determination, monitoring, and measurement along several avenues.

- ***Anomaly Detection***. NIST is working with industry to identify and demonstrate automated tools for detecting security-relevant fault conditions. In FY18, a project was *initiated* to show ways to improve detection of cybersecurity attacks in manufacturing infrastructure environments. Preliminary project findings were published for public comment as NISTIR 8219.[84] The anomaly detection activity will be expanded in FY19 to include additional detection tools.
- ***Cyber Risk Analysis (CRA) Project***. This project promotes technical solutions that enable organizations to bridge diverse, new, and existing data sets to advance analysis of cyber risks. The goal is to enable information sharing among risk owners about historical, current, and future cyber risk conditions. NIST is leveraging 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. The near-term focus is on reconstructing the University of Maryland (UMD) CyberChain Portal, which is the foundational platform for a Cyber Incident Data and Analysis Repository (CIDAR)[85] prototype. NIST is exploring the frameworks, formats, and standards that could help to automate data collection. In FY18, nearly 60 open and private cyber incident databases were reviewed. In FY19, data elements associated with the CIDAR categories will be examined for linkages that support data enrichment and bind

[84] NISTIR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*, https://csrc.nist.gov/publications/detail/nistir/8219/draft

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

to services from NIST's NVD and DHS's Automated Indicator Sharing (AIS)[86] tool. The research effort's output will be an initial proposed set of cyber incident data points with associated metrics. A common lexicon is being explored through collaboration with the Department of Defense and its DoD Cybersecurity Analysis and Review (DoDCAR)[87] program to incorporate the Open Security Controls Assessment Language (OSCAL) to support the automation of reporting for cybersecurity assessment-related information.

- ***Asset Management***. One of the immediate challenges most frequently cited by organizations is how they can establish and maintain complete records of their hardware, software, and information assets. Without knowing what hardware and software assets are in their inventories, they cannot effectively ascertain and monitor the security status of systems. NIST is collaborating with industry partners to promote the adoption of ISO/IEC 19770-2:2015,[88] which establishes a specification for representing software identification and management information, and with DHS to produce guidelines for interoperable software identification (SWID) tags (NISTIR 8060).[89] In FY18, NIST worked with the IETF to integrate SWID tags into the Network Endpoint Assessment (NEA)[90] protocol (RFC 8412),[91] helped to develop a draft software inventory message and attributes (SWIMA) specification,[92] and released project webpages[93] to provide information on tagging. In FY18, NIST also finalized a guide that shows healthcare organizations how to protect electronic health records from being exploited in a manner that endangers patient health or compromises identity and privacy (SP 1800-1).[94] NIST also released a guide that shows financial service organizations a way to more securely and efficiently monitor and manage their many information technology hardware and software assets (SP 1800-5).[95] In FY19, NIST plans to continue its SWID standardization activity and begin work on a Practice Guide for using cybersecurity mechanisms to protect systems from exploitation from internal and external network access.

[86] Automated Indicator Sharing (AIS), https://www.dhs.gov/cisa/automated-indicator-sharing-ais

[87] DoD Cybersecurity Analysis and Review, https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2018/WedPM2.2-STARCAR%20SCRM%20FINAL%20508.pdf

[88] ISO/IEC 19770-2:2015, https://www.iso.org/standard/65666.html

[89] NISTIR 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*, https://csrc.nist.gov/publications/detail/nistir/8060/final

[90] Network Endpoint Assessment (NEA), https://tools.ietf.org/html/rfc5209

[91] Software Inventory Message and Attributes (SWIMA) for PA-TNC, https://tools.ietf.org/html/rfc8412

[92] Software Inventory Message and Attributes (SWIMA), https://datatracker.ietf.org/doc/rfc8412/

[93] Software Identification (SWID) Tagging, https://csrc.nist.gov/projects/software-identification-swid

[94] SP 1800-1, *Securing Electronic Health Records on Mobile Devices*, https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices

[95] SP 1800-5, *IT Asset Management*, https://www.nccoe.nist.gov/projects/use-cases/financial-services-sector/it-asset-management

- ***Automated Combinatorial Testing***. Engineers often encounter security failures that result from unexpected interactions between components. If all faults in a system can be triggered by a combination of 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[96] are being applied to software and hardware testing for reliability, safety, and security. NIST's focus is on empirical test results and their impact on real-world problems. Advances for 2018 included the development of parallel processor code for measuring the combinatorial coverage of very large (>1,000 variables) test arrays. This tool is being applied by industry in evaluating the quality of their test suites for commercial products. In FY19, these methods will be applied to verification and testing for the Internet of Things in industrial control and home automation applications.
- ***Security Automation and Continuous Monitoring***. IT environments are under constant threat of attack and are frequently undergoing change with new and updated software being deployed along with updated configurations. The wide variety of computing products, dynamic nature of software, speed of configuration change, and diversity of threats challenges organizations to maintain situational awareness over their IT assets and utilize this information to make informed risk-based decisions. Security automation employs standardized data formats and transport protocols to enable data to be exchanged between business, operational, and security systems that support security processes. This is done by identifying IT assets, providing awareness over the operational state of computing devices, enabling security reference data to be collected from internal and external sources, and supporting analysis processes that measure the effectiveness of security controls and provide visibility into security risks, thereby enabling risk-based decision making. In FY18, 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 FY19 as NIST seeks to improve the interoperability, broad acceptance, and adoption of security automation solutions to address current and future security challenges. In turn, this will create opportunities for innovation.

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

THIS PAGE IS INTENTIONALLY LEFT BLANK