2018 ANNUAL REPORT

NIST/ITL CYBERSECURITY PROGRAM

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

NIST SPECIAL PUBLICATION 800-206

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