2016 ANNUAL REPORT

NIST/ITL CYBERSECURITY PROGRAM

NIST SPECIAL PUBLICATION 800-195

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

THIS PAGE IS LEFT INTENTIONALLY BLANK.

ANNUAL REPORT 2016

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, Inc.
Annapolis Junction, Maryland

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM
https://doi.org/10.6028/NIST.SP.800-195

SEPTEMBER 2017

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

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. § 3541 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 800-195
Natl. Inst. Stand. Technol. Spec. Publ. 800-195, 156 pages (September 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-195

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.

ACKNOWLEDGMENTS

The editors, Patrick O'Reilly of the Computer Security Division (CSD) and Kristina Rigopoulos of the Applied Cybersecurity Division (ACD), would like to thank their ITL colleagues who provided write-ups on their 2016 project highlights and accomplishments for this annual report (their names are mentioned after each project write-up). The editors would also like to acknowledge Elaine Barker (CSD), Lisa Carnahan (Standards Coordination Office, NIST), Greg Witte and Larry Feldman (G2) for reviewing and providing valuable feedback for this annual report.

The editors would also like to acknowledge Kristen Dill of Dill and Company, Inc. for designing the cover and inside layout for this 2016 annual report.

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

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

TABLE OF CONTENTS

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

TABLE OF CONTENTS

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

THIS PAGE IS LEFT INTENTIONALLY BLANK.

WELCOME LETTER

Awareness about the importance of strong cybersecurity for maintaining trust in the economy and protecting the nation is at an all-time high. So, too, are the challenges. When it comes to cybersecurity, the National Institute of Standards and Technology (NIST) has a long history of conducting path-breaking research and development, cultivating standards and best practices, and facilitating technology transitions. We rely on open, transparent, and collaborative processes that engage private and public sector participation and attract expertise from around the world. This 2016 report captures our most noteworthy accomplishments.

In 2016, NIST continued to advance fundamental research to support security and interoperability standards and guidelines. This work was led by the Computer Security Division (CSD) in the NIST Information Technology Laboratory (ITL). Among other things, CSD is responsible for developing cybersecurity standards, guidelines, tests, and metrics for the protection of non-national security federal information systems. Recognizing the agency's need to respond to and anticipate increasing demands for its cybersecurity expertise, NIST established the Applied Cybersecurity Division (ACD) within ITL to support additional applied research and to transition effective cybersecurity technology approaches to government and business sectors nationwide. ACD helps to drive the adoption of appropriate cybersecurity solutions by government and commercial organizations – enabling solutions-oriented collaborative interactions and offering guidance on the use of research results, standards, and best practices. Other parts of NIST also are key contributors to NIST's cybersecurity portfolio.

Strong partnerships with industry, academia and government are critical to NIST's cybersecurity program. In 2016, NIST continued to collaborate with stakeholders from across the country and around the world to raise awareness and encourage use of the voluntary Cybersecurity Framework. In this spirit, NIST began to develop an update to the version first published in 2014. NIST also prepared a draft Cybersecurity Framework profile aligned with manufacturing sector goals and industry best practices. In addition, NIST developed the draft Baldrige Cybersecurity Excellence Builder self-assessment tool that complements the Cybersecurity Framework and helps organizations to better understand the effectiveness of their cybersecurity risk management efforts.

Looking ahead is vital in the realm of cybersecurity. Knowing that if large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use and compromise the confidentiality and integrity of digital communication on the Internet and elsewhere, NIST is working closely with the academic community and industry to develop protective cryptographic standards that we all rely upon. Building on its successful tradition of working openly with the worldwide cryptographic community, in 2016 NIST called for submissions for quantum-resistant public-key cryptographic algorithms for standards. These algorithms must be secure against both quantum and classical computers, and should interoperate with existing communications protocols and networks. After submissions are received late in 2017, NIST plans to spend 3-5 years working with the research community and industry to analyze the candidates before selecting algorithms for standardization.

Identity management is fundamental to security management. In 2016, NIST continued to advance solutions in identity management through projects with partners who manage innovative but practical real-world solutions. Also in the past year, NIST produced an introduction to the concepts of privacy engineering and risk management for federal information systems. The goal is to help decrease privacy risks and enable organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems. NIST also initiated an update to our Digital

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195

WELCOME LETTER

Identity Guideline (Special Publication 800-63), which provides technical guidelines to agencies for the implementation of digital authentication. Building from these foundational resources, NIST's efforts will focus on strengthening the security, privacy, usability and interoperability of digital identity solutions that meet an organization's identity and access management needs throughout the system lifecycle.

During 2016, NIST's National Cybersecurity Center of Excellence (NCCoE) moved into a new permanent facility that expanded the Center's workspace from four to 23 separate, flexible laboratories—including two larger areas capable of safely hosting large equipment, such as automobiles. This additional space allows NCCoE to increase its collaborations and projects. In 2016, the Center published draft practice guides to support industry sectors, including healthcare, financial services, and energy; these guides are now beginning to be put to productive use. NCCoE also published draft documents to support security in key technology areas, such as cloud computing and mobile applications.

The National Initiative for Cybersecurity Education (NICE), led by NIST, is a partnership between government, academia, and the private sector that is focused on promoting a robust network and an ecosystem of cybersecurity education, training, and workforce development. In 2016, NIST released an update to the NICE Cybersecurity Workforce Framework (NCWF); it already is being used in the private and public sectors to more effectively identify, recruit, develop and maintain cybersecurity talent. The NICE framework provides a common language to categorize and describe cybersecurity work that helps organizations to build a strong staff to protect systems and data.

Our dedicated staff has accomplished a great deal in 2016, developing standards and working closely with scores of partners and drawing upon hundreds of private and public sector organizations and individuals. This is not a static endeavor. For example, NIST is fully aware of the urgent need to more aggressively address the security challenges of the Internet of Things and, more broadly, our connected world.

We welcome any and all suggestions about where and how we can better provide the nation with the kind of cybersecurity information and tools that it needs in order to advance and protect our economy and our country.

Donna F. Dodson,
Chief Cybersecurity Advisor

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM:
http://dx.doi.org/10.6028/NIST.SP.800-195