Full text available at: http://dx.doi.org/10.1561/110.00000010

The Economic Impacts of the Advanced Encryption Standard, 1996–2017

Other titles in Annals of Science and Technology Policy

Nanotechnology: A Call for Policy Research
Joshua Gorsuch and Albert N. Link
ISBN: 978-1-68083-498-7

The Interweaving of Diffusion Research and American Science and Technology Policy
Irwin Feller
ISBN: 978-1-68083-474-1

In Search of Evidence-based Science Policy: From the Endless Frontier to SciSIP
Albert H. Teich
ISBN:978-1-68083-444-4

Measuring Science, Technology, and Innovation: A Review
Bronwyn H. Hall and Adam B. Jaffe
ISBN: 978-1-68083-400-0

The Economic Impacts of the Advanced Encryption Standard, 1996–2017

David P. Leech
Economic Analysis & Evaluation, LLC, VA 22314, USA
david.leech@starpower.net

Stacey Ferris
RM Advisory Services, LLC, VA 22314, USA
stacey.ferris@rmadvisory.com

John T. Scott
Dartmouth College, NH 03755, USA
john.t.scott@dartmouth.edu

now
the essence of knowledge
Boston — Delft

Annals of Science and Technology Policy

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

David P. Leech and Stacey Ferris and John T. Scott. *The Economic Impacts of the Advanced Encryption Standard, 1996–2017.* Annals of Science and Technology Policy, vol. 3, no. 2, pp. 142–257, 2019.

ISBN: 978-1-68083-589-2

Annals of Science and Technology Policy
Volume 3, Issue 2, 2019

Editorial Board

Full text available at: http://dx.doi.org/10.1561/110.00000010

Editorial Scope

Topics

Annals of Science and Technology Policy publishes survey and tutorial articles in the following topics:

- Literature reviews of technology and innovation policies
- Historical case studies of technology development and implementation
- Institutional histories of technology- and innovation-based organizations
- Analyses of policies attendant to technology development and adoption and diffusion
- Studies documenting the adoption and diffusion of technologies and subsequent consequences
- Studies of public and private research partnerships (cross sectional, over time, or case based)
- Assessments and evaluations of specific technology and innovation policies
- Analyses of ecosystems associated with the technology and/or innovation development
- Cross observational (e.g., cross-agency or cross-country) comparisons of technology and innovation policies

Information for Librarians

Annals of Science and Technology Policy, 2019, Volume 3, 4 issues. ISSN paper version 2475-1820. ISSN online version 2475-1812. Also available as a combined paper and online subscription.

Full text available at: http://dx.doi.org/10.1561/110.00000010

Contents

The Economic Impacts of the Advanced Encryption Standard, 1996–2017

David P. Leech[1], Stacey Ferris[2] and John T. Scott[3]

[1]*Economic Analysis & Evaluation, LLC, VA 22314, USA; david.leech@starpower.net*
[2]*RM Advisory Services, LLC, VA 22314, USA; stacey.ferris@rmadvisory.com*
[3]*Dartmouth College, NH 03755, USA; john.t.scott@dartmouth.edu*

ABSTRACT

This paper evaluates the net social benefits of advanced encryption standards (AES), which is one of many areas where the National Institute for Standards and Technology (NIST) has promoted innovation and industrial competitiveness to ensure that public and private computer systems can protect the confidentiality, availability, and integrity of digital information in the face of ever more powerful computers and developments in the field of cryptography.

David P. Leech, Stacey Ferris and John T. Scott (2019), "The Economic Impacts of the Advanced Encryption Standard, 1996–2017", Annals of Science and Technology Policy: Vol. 3, No. 2, pp 142–257. DOI: 10.1561/110.00000010.

Full text available at: http://dx.doi.org/10.1561/110.00000010

1

Introduction[1]

1.1 NIST's mission

One of the responsibilities of the federal government is "to provide for the general welfare" (U.S. Constitution). From an economic perspective this often entails the collaboration of industry associations and state and federal agencies to mitigate barriers to economic development that arise in the normal process of innovation. It is generally understood that creation and diffusion of new technology is the single most important contributor to the nation's long-term economic growth path.[2] There is also a consensus, among economists that study the innovation process, that reliance on market processes alone will result in underinvestment in research and development, from a social point of view.[3]

[1] This monograph is an extension of an earlier NIST report, *The Economic Impacts of the Advanced Encryption Standard, 1996–2017* (NIST GCR 18-017), September 2018.

[2] Albert Link and Donald Siegel, *Technological Change and Economic Performance*, Routledge, 2003.

[3] Stephen Martin and John T. Scott, "The Nature of Innovation Market Failure and the Design of Public Support for Private Iinnovation," *Research Policy*, Vol. 29, 2000, pp. 437–447.

Toward that goal of providing for the general economic welfare, the federal government invests over $140 billion annually in R&D, a small part of which is allocated to the National Institute of Standard and Technology (NIST). These moneys are spent at NIST in an effort to fulfill its mission to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."[4]

One of many areas in which NIST has promoted innovation and industrial competitiveness is in the area of advanced encryption standards to ensure that public and private computer systems can protect the confidentiality, availability, and integrity of digital information in the face of ever more powerful computers and developments in the field of cryptography. This monograph represents a step toward evaluating the net social benefits of advanced encryption standards.

Since its creation as the National Bureau of Standards (NBS) in 1901, NIST has partnered with industry to unleash American innovation and, consequently, worldwide innovation. Over the last couple of decades, NIST's understanding of the role of technology development and innovation in the process of economic growth, the role of standards in that growth process, and how to measure NIST's contributions to innovative progress have all improved significantly.[5]

NIST serves two overarching roles in the innovation process. One is an "honest broker" role. NIST brings its respected measurement technology and expertise to innumerable scientific and commercial interactions that revolve around how the performance of new products (from cholesterol molecules and DNA fragments to light emissions and nanotubes) and processes (from the time of day and computer clock time to how fires proceed and high-rise buildings collapse) is measured and how the innovations compare with existing products and their next-generation replacements. NIST's other overarching role is as a national

[4] https://www.nist.gov/director/pao/nist-general-information.

[5] See, for example, Gregory Tassey, "Making America Great Again," *Issues in Science and Technology*," Winter 2018, pp. 72–78; and "The Roles and Impacts of Technical Standards on Economic Growth and Implications for Innovation Policy," *Annals of Science and Technology Policy*, Vol. 1, No. 3, 2017; and Albert Link and John Scott, *The Theory and Practice of Public-Sector R&D Economic Impact Analysis*, Planning Report 11-1, NIST, January 2012.

channel of the highest international standards of measurement. Scientific research, technology development, innovation, and commercialization are global phenomena and international-scale interactions that determine the performance and conformance of traded goods and services and are more important than ever to economic security.

NIST routinely directs its vast technical expertise into technology partnering activities between NIST laboratories and industries, other Federal agencies, state and local Governments, the general public, and other nations. The goal of these efforts is to enable technology transfer to promote U.S. innovation and competitiveness. Toward that end, NIST has analyzed the economic impacts of scores of NIST-performed and NIST-managed programs. Cumulatively, these impact assessments are a rich source of lessons learned for NIST laboratory managers: describing why projects were developed, what partners were involved, what problems were addressed and how, and what difference the projects made both in terms of economic impacts and NIST's stewardship of U.S. tax dollars.

1.2 Economic impact assessment focus

The focus of this retrospective economic impact assessment is NIST's AES program, which began in 1996 and continues through today; however, for the purposes of economic measurement, this monograph bounds the assessment at 2017.

The AES program was initiated as its predecessor, the Data Encryption Standard (DES) Program, was winding down. In 2000, NIST first assessed the retrospective economic impact of the DES Program.[6] The program was assessed in the context of what is now referred to as the commercial "crypto revolution."[7]

Much has changed in the world of information technology and security since 2000. Contentious policy battles over trade in cryptographic products have been resolved; stronger cryptographic algorithms are in

[6] David Leech and Michael Chinworth, *The Economic Impacts of NIST's Data Encryption Standards Program*, Planning Report 01-2, U.S. Department of Commerce/NIST, September 2001.

[7] Steven Levy, *Crypto*, Viking, 2001, p. 164.

widespread use; information security concerns that were largely ignored by much of the public are now a significant focus of public attention; powerful wireless computers are toted in the pockets, briefcases, and shoulder bags of a broad swath of the worlds' adult population; and the technology and practices employed by nefarious information system hackers have risen to the status of tangible threats to national sovereignty.

The Trump Administration's Management Agenda calls on Federal agencies to improve the transfer of Federally-funded technologies from lab-to-market and the evaluation of its economic impact.[8] For NIST, intramural R&D is an important component of that Federal funding. This economic impact assessment is intended to revisit NIST's investments in the successor to the DES Program, understand the principal dimensions of its effects, and estimate the economic impact of NIST's AES program expenditures from its inception until today.

Within this monograph, Chapter 2 (Background) provides the ABCs of cryptography as it applies to the AES and an introduction to the computer networks that employ encryption systems. It further delves into the evolution of NIST's role as the Federal Government's authority on the computer security of civilian-focused agencies, the AES competition (1997–2000), and subsequent cryptographic validation programs including what these validation programs reveal about the composition of the encryption product market.

Chapter 3 (Economic Analysis Framework) characterizes how the AES program and subsequent dependent industry standards have functioned as economic policy tools that reduced the economic barriers of the 1990s to the development, commercialization, and application of cryptographic technologies, as well as their continuing indirect role in supporting the quality of encryption systems, reducing encryption system risks, and facilitating the growth of related industries. Chapter 3 also places the AES program in an industrial organizational context by describing the economic value chain of which the AES program is a part.

[8] https://www.whitehouse.gov/wp-content/uploads/2018/04/ThePresidentsManagementAgenda.pdf, p. 47.

Chapter 4 (Economic Assessment Impact Approach) discusses the selection of pre-survey interviews with subject matter experts, the design of the survey instrument, and survey execution.

Chapter 5 (Survey Results and Findings) describes survey results, compares selected qualitative survey findings to pre-survey expectations, describes the three-tiered approach to estimating economic impact in context of actual survey results, and reports the costs of NIST's AES program, 1996–2017.

Chapter 6 (Economic Impact of AES, 1996–2017) presents the results of the three-tiered approach to estimating the overall economic impacts of the AES program.

Chapter 7 (Overall Economic Impact Assessment Conclusions) provides a summary and conclusion of the analysis.