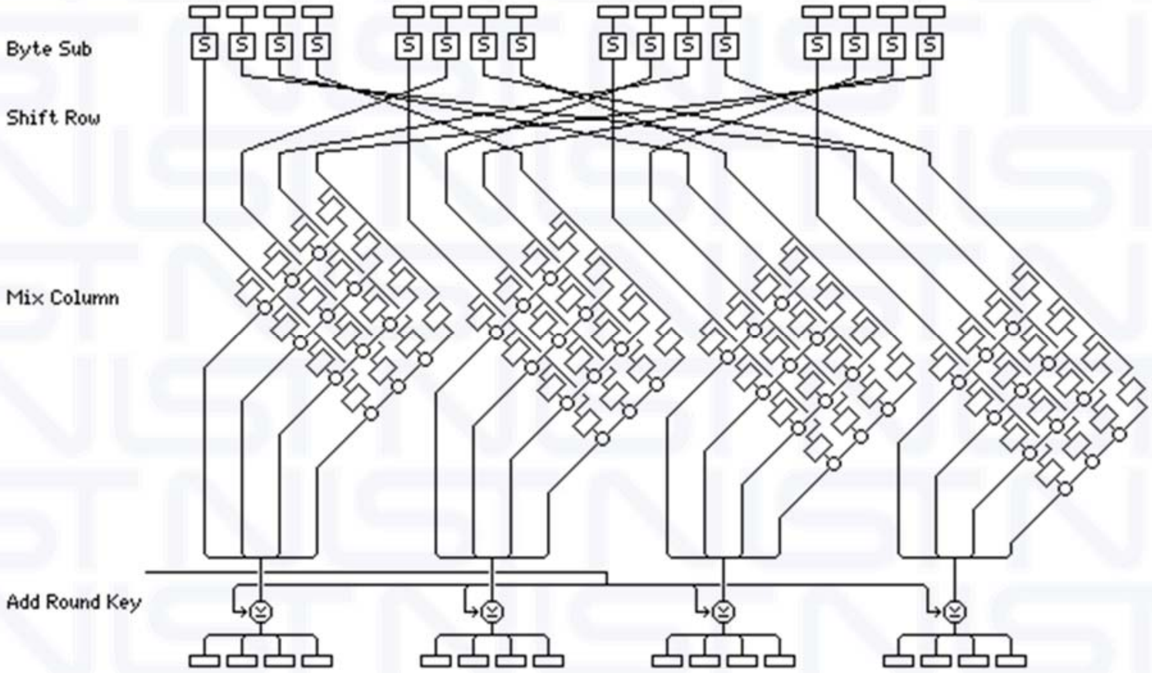
NIST GCR 18-017

# The Economic Impacts of the Advanced Encryption Standard, 1996 - 2017



David P. Leech

Stacey Ferris, CPA

John T. Scott, Ph.D.

September 2018

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

This publication is available free of charge from: https://doi.org/10.6028/NIST.GCR.18-017

**NIST GCR 18-017**

# The Economic Impacts of the Advanced Encryption Standard, 1996-2017

Prepared for
*U.S. Department of Commerce, Operating Unit:*
*National Institute of Standards and Technology, Gaithersburg, MD 20899*

*This publication was produced as part of Contract SB134117RQ0572 with the National Institute of Standards and Technology. The contents of this publication do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.*

David P. Leech
Stacey Ferris, CPA
*RM Advisory Services LLC*

John T. Scott, Ph.D.
*Dartmouth College*

September 2018

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology*

## ACKNOWLEDGEMENTS

First and foremost, we acknowledge the contributions of Dr. Eric Burger, of Georgetown University's Security and Software Engineering Research Center ($S^2$ERC), for technical advice throughout the project and especially for helping to infuse economically meaningful concepts with equally meaningful technical content during the survey design phase of the project.

Economic impact assessments occur in stages. Ultimately, we owe a great debt to many, mostly unknown, survey respondents who took the time to respond to a relatively difficult survey. The preparation and execution of the survey also owes a great deal to those who participated in background interviews as well as the efforts of several cyber-security related associations and standards development organizations that encouraged their members to participate in the survey.

Historical background information was provided by public and private sector individuals, some of whom participated in the early stages of the Advanced Encryption Standard (AES) program. They helped anchor our understanding of what was at stake in the decisions to launch the AES initiative, to participate in it, and to adopt AES-based encryption systems. Among current and former NIST personnel, we acknowledge the contributions of Larry Bassham, Lily Chen, Donna Dodson, James Foti, Edward Roback, Matthew Scholl, and Miles Smid. We would like to thank Vincent Rijmen at the University of Leuven, Belgium, one of the co-creators of the winning algorithm for AES, for his insights on AES, the competition, and the cryptographic environment of the 1990s. The following individuals provided insights from the private sector perspective: David Balenson (SRI International), John Callas (Apple), John Green (Hewlett Packard), Marc Ireland (UL Transaction Security), Brian LaMacchia (Microsoft), Lisa Yin (RC6 developer, formerly of RSA Labs), Matt Keller (Corsec), Matthew McGhee (COACT, Inc.), Ari Singer (TrustiPhi), Paul Spaven (3e Technologies International, Inc.), Ashit Vora (Acumen Security), Steven Weingart (Hewlett Packard), and others who wished to remain anonymous. Special thanks to Matt Keller who went the extra mile in providing a sounding board for numerous technology and industry issues as they arose over the course of the project.

Several associations supported the survey phase of the project by making their members aware of the project and encouraging them to respond to the survey. We thank the following individuals and their organizations for their support in this regard: Chris Cook (College of Healthcare Information Management Executives, CHIME), Patrick Gaul (National Technology Security Coalition, NTSC), Marie Gilbert (Information Systems Audit and Control Association, ISACA), Matt Keller (Cryptographic Module User Forum, CMUF, and Common Criteria User Forum, CCUF), Alex Morris (Internet Engineering Task Force, IETF), Paul Nikolich (Institute of Electrical and Electronics

Engineers, IEEE), Josh Poster (National Council of ISACs, NCI), Douglas Robinson (National Association of State Chief Information Officers, NASCIO), Eileen Sciarra (Information Systems Security Association, ISSA), Foy Shiver (Anti-Phishing Working Group, APWG), Steve Stevens (Accredited Standards Committee X9), and Lynn Terwoerds (Executive Women's Forum on Information Security, EWF).

Michael Walsh and Kathleen McTigue of NIST's Technology Partnership Office (TPO) reviewed drafts of the report and offered many helpful suggestions. Kathleen McTigue was the NIST project manager and guided the project smoothly from start to completion.

Cover page diagram of AES round transformations courtesy of John Savard.

# TABLE OF CONTENTS

## Report Tables

## Report Figures

# Executive Summary

Each year, the Federal Government spends more than $140 billion on research and development (R&D). Approximately $40 billion is used to support intramural research and Federally funded R&D centers, a relatively small portion of which goes to the National Institutes of Standards and Technology (NIST) in support of a wide array of research and technology development projects. The creation of new technology—typically a virtual partnership of public and private funding, and increasingly a formal partnership—is the single most important contributor to the nation's long-term economic growth path. Citizens and policymakers hope and expect that Federal tax dollars will be spent wisely. This study looks at the issue in a microcosm: an evaluative case study of the economic impacts of the Advanced Encryption Standard (AES) Program.

NIST's primary role in the national innovation system is the development of measurement-related know-how in support of industry, other Federal agencies, and state level agencies. NIST personnel are often called upon to act as honest brokers in industry-led standards development organizations when technological complexities, and the complexities of competing vested interests, threaten to slow progress on standards development supporting research, technology development, and the commercialization of new or upgraded products and services.

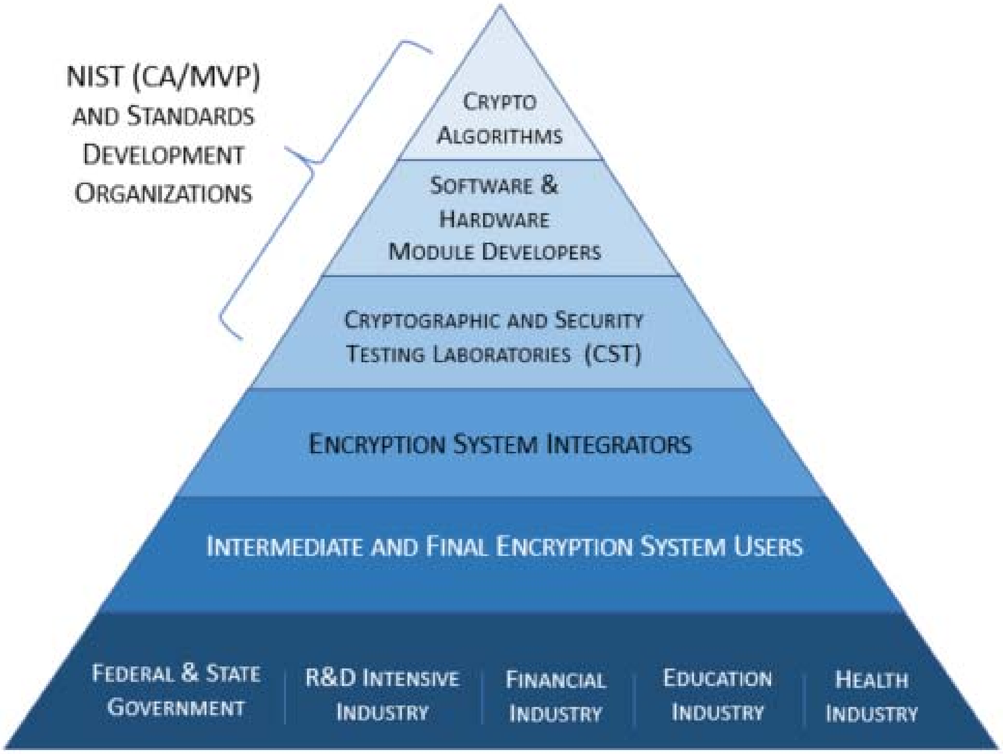
Since 1965, NIST has also been responsible for uniform Federal automatic data processing standards or Federal Information Processing Standards (FIPS). FIPS are used to provide guidance to the Federal Government for computer security, interoperability, and other information technology matters where suitable industry standards do not exist. Obviously, the role of information and information technology has ballooned since 1965 and concerns about confidential information security have risen to the status of a tangible threat to national sovereignty.

Cryptography is a branch of applied mathematics concerned with developing complex algorithms for scrambling information ("plaintext") into an indecipherable version of that information ("ciphertext") and back to plaintext. The basics of cryptography as it applies to the AES algorithm are discussed in Section 2.1, Cryptography ABCs. In 1993, the Computer Security Division (CSD) of NIST's Information Technology Laboratory (ITL) decided that the current FIPS (FIPS-46-2, Data Encryption Standard, DES, adopted in 1977) was growing vulnerable in the face of advances in cryptanalysis and the exponential growth in computing power.

This impact assessment covers the period from 1996-2017. In 1996, CSD began to plan seriously for the process that would replace DES with AES (FIPS-197), and the process for assuring conformance to AES as spelled out in the companion standard, the Cryptographic Algorithm Validation Program and the Cryptographic Module Validation Program (CAVP, CMVP, FIPS-140-2). That process—referred to in this document as the AES program—is the focus of this report.

The beneficiaries of the AES program include organizations that are part of what is depicted in Figure ES-1 as the encryption system value chain. The value chain begins with the developers of cryptographic algorithms, whose outputs are transformed into usable (and more-or-less widely used) hardware and software by the interplay of module developers, standards bodies, NIST, and testing laboratories. System integrators use these existing modules in their products, which are supplied to intermediate and final encryption system users. The five largest user sectors are the Government, private sector R&D intensive industries (protecting intellectual property), and the financial, education, and health services industries.

*Figure ES-1. The Encryption System Value Chain*


NIST (CA/MVP) and Standards Development Organizations
Crypto Algorithms
Software & Hardware Module Developers
Cryptographic and Security Testing Laboratories (CST)
Encryption System Integrators
Intermediate and Final Encryption System Users
Federal & State Government
R&D Intensive Industry
Financial Industry
Education Industry
Health Industry

Since the AES program's inception as a competition and evaluation process to identify a sufficiently strong and efficient cryptographic algorithm—a process that involved the collaboration of the worldwide cryptography community—the AES program has continued to create economic value by transferring its know-how—in many forms (e.g., the development and promulgation of "Special Publications" that specify, maintain, and revise cryptographic modes of operation)—into the network of communications and transactions that comprise this value chain.

*Table ES-1. Economic Impact of the AES program, 1996-2017*

| Economic Impact Metric | Most Conservative Outcome | Extrapolated Outcome | Economy Wide Extrapolated Outcome | Ranges for Other Infratechnology Impact Assessments |
|---|---|---|---|---|
| | (74 Survey Respondents) | (169 Survey Respondents) | | |
| Net Present Value of Benefits, 1996 (NPV96) | $844,500,000 | -- | -- | $3,500,000 - $773,000,000 |
| Net Present Value of Benefits, 2017 (NPV17) | -- | $8,772,000,000 | $250,473,200,000 | -- |
| Internal Rate of Return | 81% | -- | -- | 32-1056% |
| Alternative Internal Rate of Return | 26% | 31% | 54% | -- |
| Benefit to Cost Ratio (B/C) | 29/1 | 70/1 | 1976/1 | 3-113/1 |

Table ES-1 summarizes the quantitative findings of this economic impact analysis in terms of Net Present Value (NPV), Internal Rate of Return (IRR), Alternative Internal Rate of Return (AIRR), and Benefit-to-Cost ratio (B/C). Looking only at the column of Table ES-1 entitled "Most Conservative Outcome," based on the information discovered in the survey conducted for this project, in 1996 NIST AES program managers would have valued the AES program at $844,500,000, net of costs incurred. By comparison, of 12 other NIST infra-technology projects for which NPV was calculated (1999-2011), the median net present value was $48.5M, and ranged from $3.5M – $773M.[1]

The same logic applies to the IRR metric, the AIRR metric, and the B/C metric. A project has an acceptable economic impact if the IRR on the capital invested exceeds the cost of capital. The Executive Branch Office of Management and Budget stipulates the Government cost of capital for investment projects like AES to be 7%. Clearly the AES program's 81% IRR indicates significant impact. Similarly, a program B/C greater than one has a sufficient impact to go forward. The AES program's B/C of 29/1 (the present value of benefits/present value of costs) indicates that for every $1 of NIST's investment, society received $29 dollars' worth of cost avoidance benefits.

Explanations of the economic impact metrics based on extrapolated estimates (in the third and fourth column of Table ES-1) are discussed in the following report. Although they show significant increases in the economic impact for the AES program, they are nonetheless, as the report explains, lower bound estimates of the true economic impact of the AES program.

The opening paragraph of this executive summary observes that about $40 billion annually is used Government-wide to support intramural research. The AES program is an example of such intramural research. A very small part of that $40 billion—about $2.7 million—was spent for the AES program in 2017, close to the inflation-adjusted annual amount ($2.6 million) spent to support the program over the years from 1996 through 2017. Thus, the annual intramural Federal R&D spending for 2017 is almost

[1] For the twelve comparable NIST projects see, https://www.nist.gov/director/outputs-and-outcomes-nist-laboratory-research.

fifteen thousand times greater than NIST's annual spending for the AES program. Now consider the success of the AES program in that context and ask, "What would the annual return on investment be if the collection of Federally funded intramural R&D investments were as productive as the AES program?" For simplicity, imagine the expenditure of $40 billion annually had continued indefinitely. The annual yield on that $40 billion would have to be $72 billion to justify an internal rate of return equal to the AES program's 80%.[2]

[2] The mathematics for the internal rate of return would be the return $x$ such that $40 + 40/x = 72/x$. That internal rate of return is 0.80 or 80%.

# 1. Introduction

## 1.1 NIST's Technology Transfer Impacts Mission

Each year, the Federal Government spends more than $140 billion on research and development (R&D). Approximately $40 billion is used to support intramural research and Federally funded R&D centers, a relatively small portion of which goes to the National Institutes of Standards and Technology (NIST) in support of a wide array research and technology development projects. The creation of new technology—typically a virtual partnership of public and private funding, and increasingly a formal partnership[3]—is the single most important contributor to the nation's long-term economic growth path.[4] Citizens and policymakers hope and expect that Federal tax dollars will be spent wisely. This study looks at the issue in the microcosm of NIST's Advanced Encryption Standard (AES) Program.

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

[3] U.S. National Science Foundation, Division of Science Resources Studies, *Strategic Research Partnerships: Proceedings from an NSF Workshop*, NSF 01-336.
[4] Albert Link and Donald Siegel, *Technological Change and Economic Performance*, Routledge, 2003.
[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.

proceed and high-rise buildings collapse) is measured and how the innovations compare to existing products and their next-generation replacements. NIST's other overarching role is as a national 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 purposes of economic measurement, the study 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]

[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.

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 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, brief cases, 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 report, 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

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

industrial organizational context by describing the economic value chain of which the AES program is a part.

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 study effort.

# 2. Background

## 2.1 Cryptography ABCs

Encryption is the process of converting plaintext into ciphertext using a key. The ciphertext is only readable to key holders who can decrypt the data. Decryption translates ciphertext back to plaintext. Cryptography has become deeply interwoven in numerous facets of modern computer operations. It is "used to perform or support several basic security services: confidentiality, integrity authentication, source authentication, authorization and non-repudiation."[9] Ancient Roman ciphers were simple and limited to written alpha-numeric characters, but modern cryptographic functions performed by computers can translate any data that can be expressed in computer code, i.e., binary (1's and 0's), into unreadable ciphertext. In simple terms, encryption and decryption is the process of a computer conducting a highly complex math problem—a problem so complex that it could not be done even using computer speed, processing, and memory capacity without the key.

The two broadest categories of encryption systems are symmetric "secret-key" encryption and asymmetric "public-key" encryption. Symmetric secret-key encryption uses a single key known to both the sender and recipient for encryption and decryption. One of the greatest cryptography challenges in the 20th century was unravelling how to exchange secret keys when the sender and recipient are unable to physically meet. This puzzle was cracked in the 1970s by researchers at Stanford and the Massachusetts Institute of Technology (MIT, and the eventual founders of RSA Labs) and came to be known as public-key encryption.[10] Today, secret keys are typically encrypted using public-key encryption. Asymmetric public-key encryption makes two different keys: one public and one secret. The public key is openly available, so an authorized user can access this key to send an encrypted message to the private-key holder or verify the private-key holder's signature using their public key.

[9] Elaine Barker, *Recommendation for Key Management, Part 1: General,* NIST Special Publication 800-57 Part 1, Revision 4, 2016.

[10] The history is recounted in detail in Steven Levy, *Crypto,* Viking, 2001. As explained therein, the private-sector researchers had independently rediscovered public-key cryptography that had actually been invented in the late 1960s and early 1970s by Government researchers within the British Communications Electronics Security Group (CESG) of the Government Communications Headquarters (GCHQ)—the British counterpart to the United States' National Security Agency (NSA), but the British intelligence agency had suppressed the discovery, keeping it a secret.

For a majority of internet and network-based computer interactions, public-key encryption is used to establish a secure connection and verify computer/user identities, and secret-key encryption like AES is then used for bulk-data encryption. Symmetric secret-key cryptography can be further categorized as either stream ciphers or block ciphers, referring to whether data is encrypted one bit at a time or it is compiled into "blocks" of data that are encrypted in batches. AES is a symmetric block cipher.

Symmetric block ciphers organize plaintext data in blocks. The blocks can be visualized like the face of a Rubik's Cube with two bits of data in each square. Just as a Rubik's Cube with more blocks on each side is more difficult to solve, so a larger block in encryption increases the complexity of the mathematical functions. The block size of DES was 56-bits. AES more than doubles that and uses a block size of 128-bits.

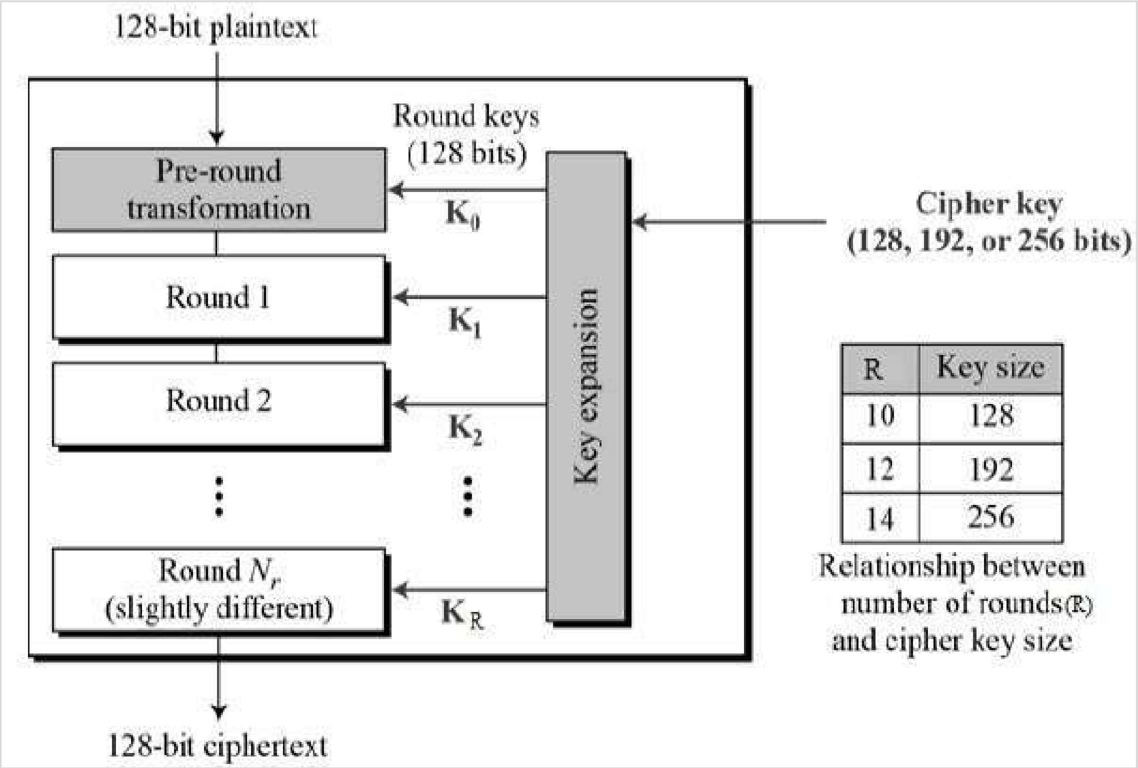
The key is also arranged as a block and used to perform mathematical scrambling functions on the plaintext data to produce cipher text. The key itself is also subject to mathematical scrambling to create versions of it. Use of multiple keys speed up encryption and increase the security when processing large amounts of data. The creators of AES described it thusly: "A block cipher transforms *plaintext* blocks of a fixed length $n_b$ to *ciphertext* blocks of the same length under the influence of a cipher key *k*."[11]

The diagram below (Figure 2-1) provides a general understanding of how AES functions.[12] Each round performs mathematical scrambling using the key, which is a set of randomly generated alphanumeric characters organized like the data. The number of rounds performed depends on the key size, as shown in the box to the right where "R" stands for "rounds." For a 128-bit key, 10 rounds of scrambling are performed; for a 192-bit key, 12 rounds of scrambling; and for a 256-bit key, 14 rounds of encryption scrambling occur.

[11] Vincent Rijmen and Joan Daemen, *The Design of Rijndael, AES—The Advanced Encryption Standard.* Springer-Verlag publishing, 2002, p. 23.

[12] http://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

*Figure 2-1. How the AES Algorithm Works*



| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Relationship between number of rounds(R) and cipher key size

Cryptographic strength increases with longer keys and larger block sizes. The key is a string of alpha-numeric characters. Designed in the early 1970s, DES had 56-bit keys, which translated to roughly 72 quadrillion (72,000,000,000,000,000) possible keys. AES has key size options of 128, 194, and 256, providing for various levels of security. For most applications, 128-bit keys are employed. During the period covered by this study of 1996-2017, the U.S. National Security Agency (NSA) approved AES-256 as acceptable for protecting up to top-secret classified data; by comparison, DES was approved for protecting unclassified, sensitive data. The smallest 128-bit key size of AES has 2^128 possible keys, or approximately:

340,000,000,000,000,000,000,000,000,000,000,000,000 possible keys.[13]

Brute force cracking AES is widely considered unfeasible due to the immense time and computer processing resources needed to cycle through possible keys. To date, AES has not been successfully attacked in this manner and it is generally held by NIST and the

[13] This number is pronounced “three hundred forty undecillions.” http://www.webmath.com/_answer.php

cryptographic community that even quantum computers will not, in the near term, be able to brute force crack data secured by AES-256.[14]

At a high level, breaking a cipher can be done one of two ways: either run through key options until the correct key is found (brute force attacks), or perform cryptanalysis, that is, pattern and probability analysis to guess plaintext-ciphertext pairs and decrypt from there. Block ciphers arrange data in blocks for encryption. Longer chains of data with thousands of blocks hold an increased risk of having two identical blocks, which increases the susceptibility to cryptanalysis. DES became susceptible to both types of attacks. The AES developers noted that, “resistance against these two attacks is the most important criterion in the design of Rijndael.”[15] Various modes of operation available with AES address this potential weakness by performing additional block setup steps to reduce the probability of inadvertent duplications or other weaknesses.

AES can operate in five different confidentiality modes: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes.[16] The mode used will depend upon the specific implementation of encryption and how keys are generated, stored, and validated. The AES modes of operation were implemented with an eye towards covering any potential weak points that would create analyzable information. The modes of operation available in an encryption hardware or software unit are determined when the AES code is implemented. Multiple modes can be available for use in one module, and they are selected based on the nature of the data that will be encrypted and decrypted.

Modes of operation can be thought of metaphorically: A person dresses according to the anticipated weather. If it is going to be sunny and warm, the person will not wear a jacket. If it will be windy and rainy, they will wear a jacket and bring an umbrella. The person is like AES and does not change, but what the person is wrapped or dressed in—that is, the person’s “mode of operation”—does change according to the anticipated

[14] Lily Chen, et. al., *Report on Post-Quantum Cryptography* (NISTIR 8105 DRAFT), February 2016, p. 3. (Re., symmetric key systems, “We don’t know that Grover’s algorithm will ever be practically relevant, but if it is, doubling the key size will be sufficient to preserve security.”)

[15] Rijmen and Daemen, op. cit., p. .81.; Rijndael is the name of the cipher chosen for the AES.

[16] https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Current-Modes

weather, or for AES, its modes of operation are set based on the anticipated data it will encounter.

## 2.2 Elements of an Encryption System

This study defines “encryption systems" to be information systems that use hardware and software modules to perform core encryption processing, key generation, key management, and any other secure data storage and transmission. Encryption system engineers denote two types of data that can be secured via encryption:

1. **Data at rest**, or stored data: data resident on a device (e.g., a hard drive or smartphone) that are neither being manipulated nor otherwise processed.
2. **Data in motion**, or data in transit: data being sent between various points.[17]

Data is held, processed, and transmitted by a variety of hardware and software modules. *Encryption hardware* includes storage devices, network appliances, standalone encryption engines and accelerators, access and authentication systems, radios, and telephones. *Encryption software* includes cryptographic libraries, developers’ toolkits, dedicated software encryption processors or accelerators, dedicated software key management, authentication system interfaces, virtual network routers, switches, and firewalls, and virtual network management software.

Figure 2-2 depicts a typical encryption system for cloud hosting, data centers, and other large data processing/holding operations. Within this figure, the end user terminal sends requests or data to remote servers. The remote servers handle thousands of requests per minute, so they offload key generation and some encryption work to dedicated encryption units to achieve processing efficiencies.

[17] Chris Jaikaran, *Encryption: Frequently Asked Questions*, Congressional Research Service, September 28, 2016.

*Figure 2-2. Large Encryption System*

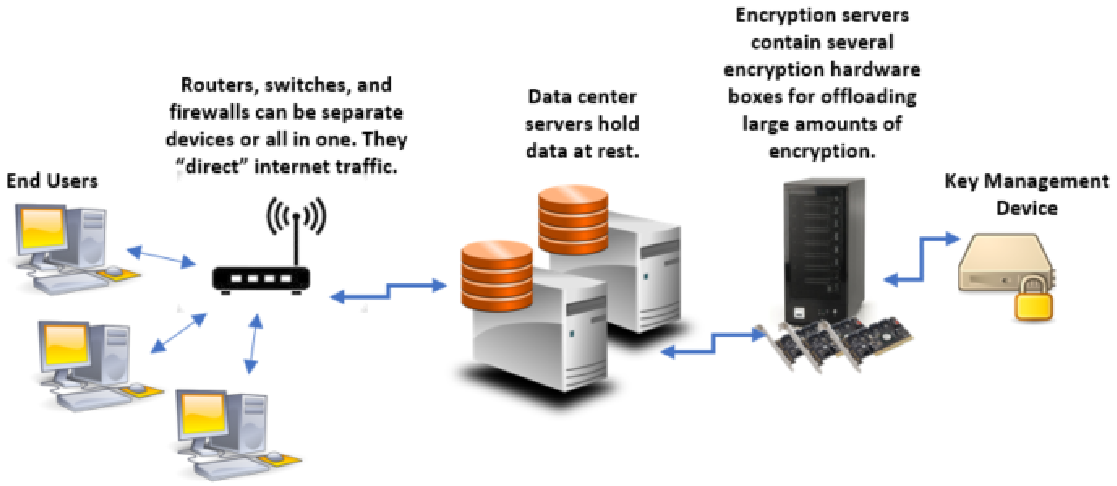
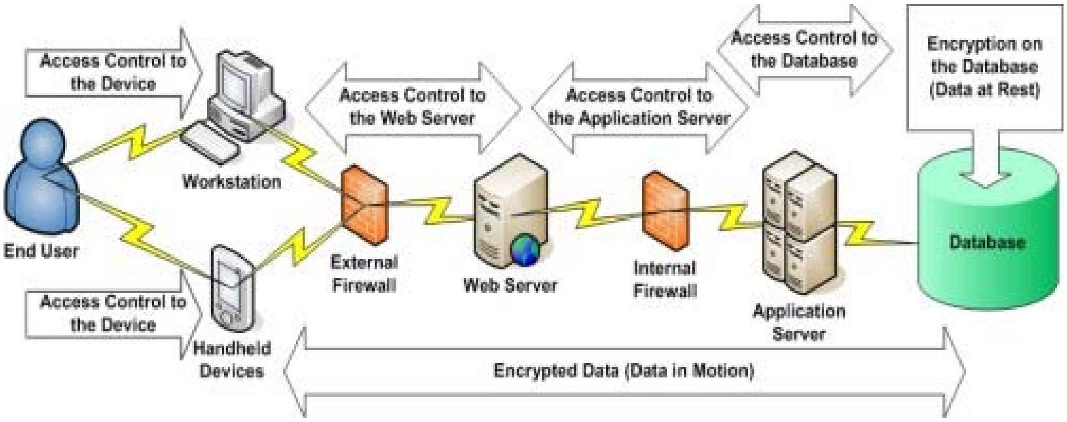

End Users
Routers, switches, and firewalls can be separate devices or all in one. They "direct" internet traffic.
Data center servers hold data at rest.
Encryption servers contain several encryption hardware boxes for offloading large amounts of encryption.
Key Management Device

Figure 2-3 illustrates use of encryption for access controls in a smaller encryption system. In this small-scale encryption system, all encryption processing is performed within the devices and no work is offloaded. As an encryption system gets smaller, it will compress and shrink encryption processes into as few discrete hardware and software modules as possible to increase speed and efficiency. Figure 2-3 depicts the end user as using either a computer or handheld device; however, the array of devices captured by the phrase "Internet of Things" has the potential to extend an encryption system beyond the end-user terminal and network infrastructure to include such items as home appliances, vehicles, wearable technology, bridges, railway tracks, onshore and offshore wind-farms, and the like.

*Figure 2-3. Small Encryption System*[18]


Access Control to the Device
Workstation
End User
Access Control to the Device
Handheld Devices
Access Control to the Web Server
External Firewall
Web Server
Access Control to the Application Server
Internal Firewall
Access Control to the Database
Application Server
Encryption on the Database (Data at Rest)
Database
Encrypted Data (Data in Motion)

[18] Source: https://www.cdc.gov/cancer/npcr/tools/security/encryption2.htm

## 2.3 The U.S. Encryption Regulatory Environment

Federal Information Processing Standards, or FIPS, were born in the Brooks Act of 1965 and evolved with the changing roles of the Department of Commerce and NIST over time. Congressman Jack Brooks, the chairman of the Government Activities Subcommittee of the Committee on Government Operations of the House, introduced the Brooks Bill (H.R. 4845) in 1965 to amend Title I of the Federal Property and Administration Services Act of 1949 to correct known deficiencies in government automated data processing management, one of which was a lack of standardization and compatibility. What came to be known as "the Brooks Act" (Public Law 89-306, 1965) is regarded as the earliest significant congressional action affecting Federal use of information technology.[19] It assigned authority to the Department of Commerce to make recommendations for uniform Federal automatic data processing standards.[20] Implementation of the act called for a new publication series of automatic data processing standards, to be called Federal Information Processing Standards Publications, "FIPS PUBS."[21]

FIPS have arguably grown in stature and importance over time, particularly as computer-based technology finds its way into every aspect of both public and private sector operations. NIST's role as an honest broker in developing FIPS has brought both domestic and international industry and academia to the table.

NIST first tackled symmetric block encryption with FIPS-46, the Data Encryption Standard (DES), published in 1977. DES dominated the 1980s when encryption was still primarily considered a national security and defense concern. In a 1988 survey study, the Government Accountability Office (GAO) reported 97% of all reported sensitive systems, or approximately 52,000 sensitive Government systems, were within the

[19] U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Management, Security, and Congressional Oversight, OTA-CIT-297 (Washington, D.C.: U.S. Government Printing Office, February 1986).

[20] Charles I. Willis, *The Brooks Act, is it Relevant Today?* (Masters Thesis) Naval Postgraduate School, June 1994, pp. 8-13; Public Law 89-306, October 30, 1965. *An act to provide for the economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing equipment by Federal departments and agencies.*

[21] Elio Passaglia, *A Unique Institution: The National Bureau of Standards 1950-1969,* U.S. Government Printing Office, 1999, pp. 558-560.

Department of Defense (DoD). It comes as no surprise then that the NSA, the intelligence agency founded to create and unravel WWII encrypted communications, was heavily involved in encryption algorithms design and use in the Federal space.

From the 1950s through the 1990s, the NSA was the dominant voice in Federal cryptographic regulation matters. The agency advocated for the export limits of encryption to be set at 40-bit keys, under the conviction that encryption was a matter of national security. Indeed, the primary users of encryption for much of the 20th century were national security-related entities. Even DES with its 56-bit keys was considered too strong for export, and thus IBM (the DES creator) also developed a weaker 40-bit key version for use in exported hardware and software.[22] The NSA had worked closely with IBM on the development of DES, and reportedly made some unexplained changes to the nature of the S-boxes used in the block cipher.[23] As a consequence, the reputation of DES suffered in the eyes of many commercial players due to the shrouded involvement of the NSA in its development.

In the DES era, responsibility for computer security was spread among a number of agencies including the DoD, NSA, General Services Administration (GSA), and the National Bureau of Standards (NBS, later NIST). A report by the House of Representatives, Committee on Science, Space, and Technology, accompanying the Computer Security Act (CSA) of 1987, worried that a “lack of coordination” weakened U.S. computer security policy:

> This mixture of laws, regulations, and responsible agencies has raised concern that Federal computer security policy is lacking direction and forcefulness in some areas, yet has created overlapping and duplication of effort in other areas.[24]

[22] https://en.wikipedia.org/wiki/Data_Encryption_Standard#cite_note-6

[23] In the description of how encryption works, the S-boxes were likened to the faces of a Rubik’s Cube. Encryption setup involves organizing data into these boxes. The NSA’s involvement and sometimes specific insistence on certain design elements fueled private sector fears that there was an intentional Government “backdoor” in the DES algorithm. General sentiment suggests that NIST successfully avoided this with AES by hosting a public and global AES competition.

[24] https://csrc.nist.gov/csrc/media/projects/ispab/documents/csa_87.txt

The CSA of 1987 attempted to redress this situation by moving responsibility for computer security to the agency level and consolidating more authority under the Department of Commerce. It required Federal agencies to identify systems with sensitive information and provide training on security measures to employees. However, it provided limited direction on how to define a sensitive system and what constituted sufficient training and security measures. A 1988 GAO audit of Federal compliance with the CSA indicated unequal and uncoordinated efforts across agencies as they developed their own internal criteria for identifying sensitive systems and providing training and security.[25]

The 1990s heralded the introduction of the World Wide Web to the greater public, and excitement around this new technology fueled rapid economic expansion in computer technology. Certainly, by the time the 21st century dawned, there was tremendous national excitement and energy around computer technologies. Federal agencies and the technology companies that served them were anticipating the new AES. The controversy over export policy continued to rage even as the AES project was launched in 1996. The controversy was not resolved, so far as the export market was concerned, until 2000 when the newly in charge Department of Commerce, Bureau of Export Administration, significantly relaxed restrictions on cryptographic hardware and software products by "multilaterally decontrol[ling] mass market encryption commodities and software up to and including 64-bits… making them eligible for export and re-export to all destinations."[26] As commercial mass-market products using AES began rolling out in the following years, they were eligible for export. The AES source code was made freely available worldwide, and over time has become a trusted algorithm across the globe.[27]

In July 2001, the e-Government Act was introduced to Congress, which evolved into the 2002 Federal Information Security Management Act (FISMA). FISMA recognized that the Government needed a stronger framework for operating within the emerging Internet

[25] U.S. General Accounting Office, *Computer Security: Status of Compliance with the Computer Security Act of 1987,* September 1988. GAO/IMTEC-88-61BR. https://www.gao.gov/assets/80/77177.pdf
[26] https://epic.org/crypto/export_controls/finalregs.pdf. Rule amendments for the Bureau of Export Administration, January 10, 2000. RIN 0694-AC11.
[27] AES is included in European and Japanese Government recommended encryption algorithm lists, among others.

and digital technology spaces. Most significantly, FISMA prohibited agencies from waiving compliance with computer security measures, which was permitted under previous legislation. FISMA also required NIST to do the following:

- Establish standards for categorizing information and information systems according to ranges of risk-levels (See FIPS-199 and -200);
- Develop minimum security requirements for information and information systems in each of the risk categories;
- Develop guidelines for detection and handling of information security incidents; and
- Develop guidelines, in conjunction with the DoD, for identifying an information system as a national security system.[28]

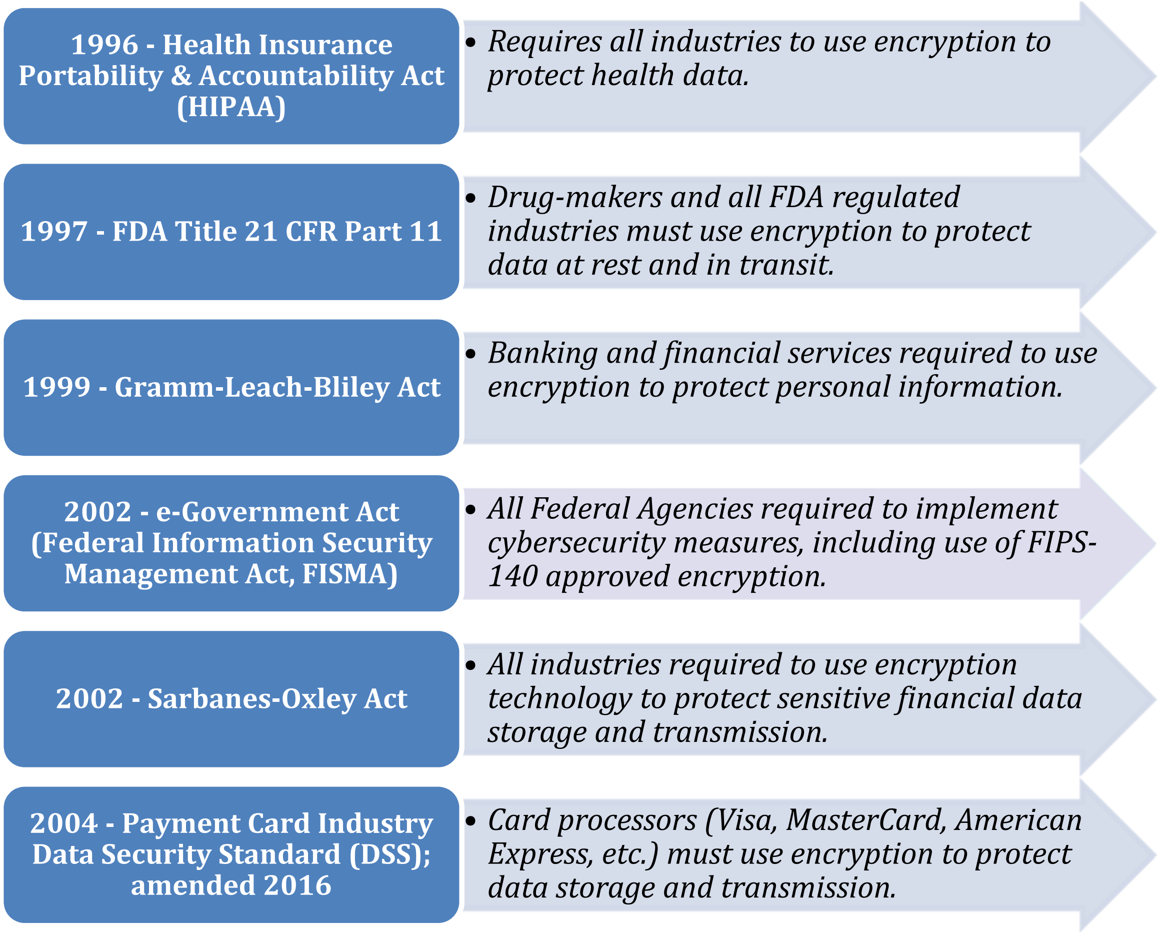
In 2004, the GAO issued guidance for FISMA compliance that highlighted cryptography as an "integral part of an effectively enforced information security policy."[29]

Beyond the Federal Government, laws and regulations passed between 1996 and 2004 specifically called for the use of encryption in the financial, healthcare, and retail industries, as well as in all publicly traded companies. The most significant of these laws and regulations are highlighted in Figure 2-4. In turn, these industries and companies looked to established industry standards for guidance. Industry standards bodies often reference FIPS and use them as a foundation for industry specific standards; however, the only entities required by Federal law to use certified FIPS ciphers are Federal Government agencies.

As a result of increased legislation, relaxed encryption export regulation, and the sheer volume of buying power that the Federal Government possesses, FIPS standards have influenced nearly every sector of the U.S. economy in some way.

[28] *Federal Information Security* (GAO 17-549), United States Government Accountability Office, September 2017.
[29] *Information Security: Technologies to Secure Federal Systems*, GAO-04-467, March 2004.

*Figure 2-4. Laws and Regulations Requiring Use of Encryption by the Private Sector*



**1996 - Health Insurance Portability & Accountability Act (HIPAA)**

- *Requires all industries to use encryption to protect health data.*

**1997 - FDA Title 21 CFR Part 11**

- *Drug-makers and all FDA regulated industries must use encryption to protect data at rest and in transit.*

**1999 - Gramm-Leach-Bliley Act**

- *Banking and financial services required to use encryption to protect personal information.*

**2002 - e-Government Act (Federal Information Security Management Act, FISMA)**

- *All Federal Agencies required to implement cybersecurity measures, including use of FIPS-140 approved encryption.*

**2002 - Sarbanes-Oxley Act**

- *All industries required to use encryption technology to protect sensitive financial data storage and transmission.*

**2004 - Payment Card Industry Data Security Standard (DSS); amended 2016**

- *Card processors (Visa, MasterCard, American Express, etc.) must use encryption to protect data storage and transmission.*

## 2.4 The Genesis of AES

### 2.4.1 Prelude to AES: It was not always thus

In historical context, the AES competition was a remarkable event as it followed two decades of acrimony between the commercial sector's efforts to cash in on the developments of private sector cryptographic innovation, and the efforts of largely secret government agencies trying to gain control of cryptography as their sole province in the post-WWII era. Those agencies were initially exposed to the wider public—and many budding civilian cryptographers—by academic and other independent critics, for example, in workshops organized by NIST in the 1970's to review the draft of FIPS-46.[30]

[30] Levy, op. cit., pp. 56-65.

NIST straddled that divide for a long time, beginning with Brooks Act of 1965. As early as 1993, NIST noted that DES was increasingly not up to par for the demands put upon it by computer technology utilized at the time. It was evident that if computer power continued to increase at a steady pace, DES would be outdated and unusable by the end of the decade. Indeed, by the end of the 1990s, cryptanalysts had demonstrated that DES could be hacked in less than 24 hours.[31] In 1993, NIST reviewed and reaffirmed DES for another five years (FIPS-46-2), but with a warning that it would not be reaffirmed in 1998. In 1999 Federal agencies and their suppliers and contractors were advised to begin implementing Triple DES (TDES) until an advanced encryption algorithm was developed.[32]

In essence, TDES simply runs DES three times in a row using two or three unique keys. However, if a gate is ineffective, putting up two more gates does not stop intruders, it merely delays them. Similarly, TDES delays all encryption processes, including encrypting and decrypting activities. Nonetheless, TDES remains in use today, and in fact, 3-Key TDES is approved by NIST through approximately 2030.[33]

In the mid-1990s, the Clinger-Cohen Act noted that FIPS standards were often duplicative of existing industry standards. NIST declared, “We will issue FIPS only where there are compelling Federal Government requirements.”[34] Considering that there were already several block cipher alternatives to DES at the time—such as Blowfish, IDEA, and RC5—why would NIST open a competition to create a new algorithm and FIPS? Individuals working in the mid-1990s commented that the atmosphere was one of confusion and lack of interoperability. None of the alternatives had been able to establish itself as a significantly better option than DES or TDES. As such, NIST determined that a sufficient industry standard for symmetric block encryption did not exist, and that NIST leadership, in the form of a new FIPS, was required.[35]

[31] In 1997, an RSA Labs cryptanalysis challenge team successfully brute force attacked DES after running through 25% of the 72 quadrillion keys or about 18 quadrillion keys. In 1999, another cryptanalysis team used a network of almost 100,000 PCs connected through the Internet to crack DES in 22 hours and 15 minutes. http://www.tjscott.net/crypto/des.hack.htm

[32] Miles Smid, “Developing the Advanced Encryption Standard,” mimeo, February 2, 2018, p. 4.

[33] Barker, 2016, op. cit., pp. 55-56.

[34] *Information Technology Laboratory Technical Accomplishments 1996* (NISTIR 5938), U.S. Department of Commerce, January 1997, pg. 7.

[35] Smid, op. cit.

### 2.4.2 Competition and Criteria

Anticipating the need for high-quality cryptography, in 1996 the Computer Security Division (CSD) of NIST's Information Technology Laboratory (ITL) initiated planning the development of new advanced cryptographic algorithm standards for encryption, digital signatures, and key exchange.[36] In the September 1997 Federal Register, NIST solicited submissions for the Advanced Encryption Algorithm, which would be "an unclassified, publicly disclosed encryption algorithm available royalty-free worldwide that is capable of protecting sensitive Government information well into the next century."[37] The solicitation set out three minimum acceptability requirements for candidates to be considered "complete and proper":

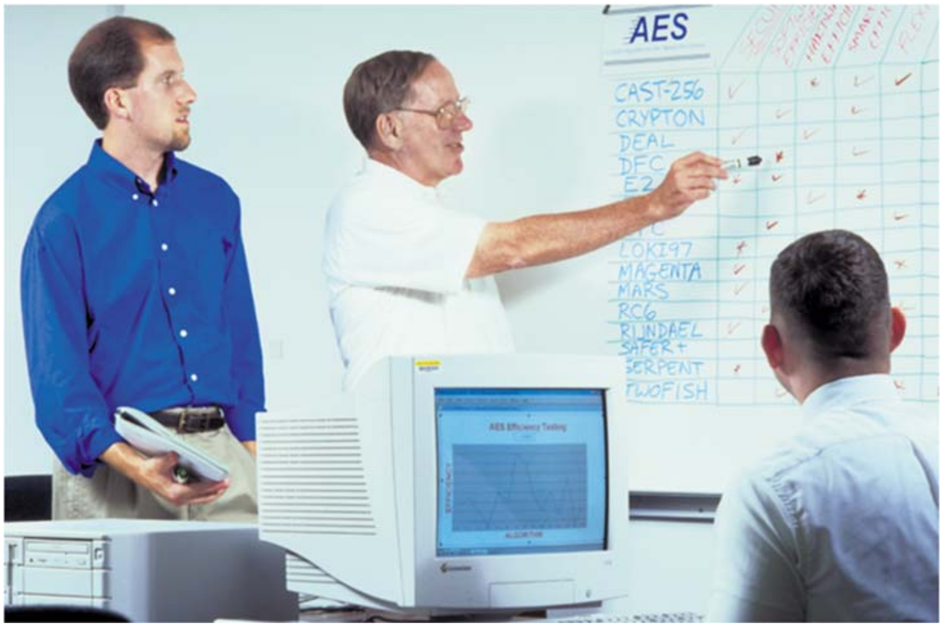
1. The algorithm must implement symmetric (secret) key cryptography.
2. The algorithm must be a block cipher.
3. The candidate algorithm shall be capable of supporting key-block combinations with sizes of 128–128, 192–128, and 256–128 bits.

Submissions would be evaluated on overall security, speed, and implementation characteristics across a variety of hardware and software (as depicted in Figure 2-5). Further, the announcement specified that the competition would involve public comment rounds to openly critique candidates as well as unearth any potential intellectual property or other conflicts. The winning algorithm would be made publicly available and royalty free upon selection.

[36] U.S. Department of Commerce, January 1997, op. cit., p. 14.

[37] *Federal Register*, September 12, 1997, "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard, A Notice by the National Institutes of Standards and Technology," Document Citation: 62 FR 48051. Document Number: 97-24214.

*Figure 2-5. NIST Experts Analyze the AES Candidates*



J. Foti, M. Smid, and E. Roback analyze the cryptographic algorithms under consideration for the Advanced Encryption Standard, 1999[38]

Candidate algorithms poured in from around the globe: the United States, Europe, Asia, and Latin America all had submissions. In total, NIST received 21 submissions that were presented at a public conference in 1998. During the conference, the submissions were openly challenged and evaluated, and six were eliminated. Fifteen submissions, shown in Table 2-1, were deemed to meet the minimum acceptability requirements. NIST's James Foti said of the decision to open the competition to international submissions, "We worked really hard to consider the public perception of what we were doing."[39]

[38] *1999 ITL Technical Accomplishments* (NISTIR 6365), NIST, October 1999, pg. 12.

[39] https://gcn.com/Articles/2001/06/28/NIST-goes-public-to-keep-Federal-secrets.aspx.

*Table 2-1: AES Competition Candidate Algorithms*

| | Algorithm | Submitter(s) | Submitter Type | Country(ies) |
|---|---|---|---|---|
| Finalists | **Rijndael** | **Daemen and Rijmen** | **Researchers** | **Belgium** |
| | Serpent | Anderson, Biham, Knudsen | Researchers | UK, Israel, Denmark |
| | Mars | IBM | Company | USA |
| | RC6 | RSA | Company | USA |
| | Twofish | Counterpane | Company | USA |
| Other Candidate Algorithms | CAST-256 | Entrust | Company | Canada |
| | Crypton | Future Systems | Company | South Korea |
| | DEAL | Outerbridge, Knudsen | Researchers | USA, Denmark |
| | DFC | ENS-CNRS | Researchers | France |
| | E2 | NTT | Company | Japan |
| | Frog | TecApro | Company | Costa Rica |
| | HPC | Schroeppel | Researcher | USA |
| | LOKI97 | Brown et al. | Researchers | Australia |
| | Magenta | Deutsche Telekom | Company | Germany |
| | SAFER+ | Cylink | Company | USA |

Qualified submissions were further evaluated on three factors: security, cost, and implementation flexibility. The security factor was deemed the most important, covering "resistance of the algorithm to cryptanalysis, soundness of its mathematical basis, randomness of the algorithm output, and relative security as compared to other candidates." The cost factor included "licensing requirements, computational efficiency (speed) on various platforms, and memory requirements"—all aspects more important to hardware implementations than software. Finally, the algorithm needed to display certain characteristics including "flexibility, hardware and software suitability, and algorithm simplicity."[40]

The candidate algorithms were analyzed on ANSI C and JAVA$^{TM}$ implementations. The ANSI C implementations "focused on speed… on various desktop systems, using different combinations of processors, operating systems, and compilers." The JAVA$^{TM}$ implementations were tested for "speed and memory usage on a desktop system".[41]

[40] James Nechvatal, et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, Computer Security Division, Information Technology Laboratory, NIST, October 2, 2000, pp. 9-11.
[41] Ibid., p. 11.

### 2.4.3 Down-Select and Worldwide Cryptanalysis

NIST encouraged participation from industry, academia, and government experts both as submitters and in public comment rounds. NIST's ITL hosted two public conferences, the first in Ventura, CA in 1998 and the second in Rome, Italy in 1999, to encourage open participation in the evaluation process. The first conference allowed the 15 accepted submitters to "formally present their candidate algorithms and design philosophy" as well as allow for open discourse and analysis of the submissions. NIST established "electronic discussion pages for each candidate" to allow for discussion of the algorithms prior to any submission of formal comments or feedback to NIST.[42]

During NIST's evaluation of the five AES finalists, Rijndael emerged as distinctly fast and efficient with "a low ROM requirement and very low RAM requirement. Both encryption and decryption are at least twice as fast as any other finalist."[43] While it ranked lower on inherent security than other competitors, it was simpler and more cost effective to implement across a range of software and hardware. Rijndael's simple structure relied only on "Boolean operations, table lookups, and fixed shifts/rotations," which were determined to be "the easiest to defend against attacks."[44] At the time, NIST observed that Rijndael's speed decreased on 192-bit and 256-bit tests; however, significant improvements in computing power have since made AES-256 a feasible option for a wide range of devices and implementations.

As part of the evaluation, NIST solicited comments from "industry, academia, standards bodies, and the public" in order to "narrow the field of candidate algorithms to five or fewer."[45] Based on the comments and feedback, five finalists, shown in Table 2-1, were chosen and subjected to more intensive testing and scrutiny, as well as a second round of public comments from August 1999 through May 2000.

[42] Edward Roback and Morris Dworkin, "Conference Report" (First Advanced Encryption Standard (AES) Candidate Conference, Ventura, CA, August 20-22, 1998), *Journal of Research of the National Institute of Standards and Technology*, Vol. 104, No. 1, January – February 1999.
[43] Nechvatal, et al., 2000, op. cit., p. 40.
[44] Ibid., p. 66.
[45] *1998 ITL Technical Accomplishments* (NISTIR 6254), NIST, October 1998, p. 14.

### 2.4.4 Final Selection

In October 2000, NIST published a whitepaper detailing the five finalists and the results of the competition evaluations. The paper nominated Rijndael to become the Advanced Encryption Algorithm and detailed the results of analysis in the three primary categories of strength, speed, and implementation flexibility.

**Strength**

The strength of an encryption algorithm is described in terms of its security margin. The security margin "indicates the resistance of the cipher against improvements of known types of cryptanalysis."[46] MARS, Serpent, and Twofish all received security ratings of "high," while RC6 and Rijndael received "adequate" security margin ratings. The evaluators found Rijndael difficult to evaluate because it had three different key sizes: 128, 192, and 256. Some expressed concern that Rijndael's relatively simple structure created cryptanalysis vulnerability; however, the same simplicity also made Rijndael "the easiest to defend against attacks" as well as making it significantly faster than the other candidates.[47]

**Speed**

One of the major factors in evaluating a cipher's speed is the rate at which it can calculate and apply a key schedule. When encrypting large amounts of data, multiple variations of the original key are used. These variations are contained in a key schedule, which is determined at the point encryption is initiated. Key schedule set up and key generation are therefore core components of cipher operation. For encryption, decryption, and key setup, the evaluators described MARS as an average performer, Serpent was low-end performance, Twofish varied across platforms but had low-end key setup, RC6 had average to high-end performance, and Rijndael consistently had high-end performance.

**Implementation Flexibility**

Implementation configurations matter since "doubling the size of an encryption program may make little difference on a general-purpose computer with a large memory, but doubling the area used in a hardware device typically more than doubles the cost of the device."[48] Selecting an algorithm with low memory requirements was preferable.

[46] Rijmen and Daemen, op. cit., p. 63.
[47] Nechvatal, et al., op. cit., p. 66.
[48] Nechvatal, et al., op. cit., pg.41

Broadly, MARS, RC6, and Serpent were deemed too slow and demanding on random access memory. Twofish was faster than these but had a high memory requirement. Rijndael had the lowest memory requirement and ran significantly faster than the other candidates.

The following year of 2001 entailed NIST developing detailed implementation guidance and operational modes (AES has five modes which vary depending on the implementation environment). In early 2001, NIST released a draft FIPS-197 for comments. The official FIPS-197 formally selecting Rijndael as the AES was published in December 2001. Some thought that the AES should include multiple algorithms, and NIST briefly considered including both Rijndael and Serpent; however, the decision to only have one algorithm with different key sizes was to "decrease the complexity of implementations" and to have the effect of "lowering costs and promoting interoperability."[49]

NIST's October 2000 report on the five competitor algorithms described the significant challenge of predicting future technology and selecting an algorithm that would serve well for decades. Since they desired an algorithm that could last several decades, adaptability to and flexibility for a variety of platforms was paramount. In the 16 years since the release of AES, computer technology has expanded rapidly across platforms, applications, and hardware, from smart phones and virtual reality to cloud computing, self-driving cars, and big data analysis. A single laptop can hold the computing power of a mainframe computer center of earlier decades. In recent years, the economy has witnessed explosive growth of e-commerce, cryptocurrency mining and markets, online gaming and social networks, and quantum computing, which is now in its infancy and anticipated to come to market around 2030.

According to Kevin Curran, a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and a professor of cybersecurity at Ulster University:

> When quantum computing becomes a reality, many public-key algorithms will be obsolete… However, encryption schemes like AES, with large keys,

[49] Faranak Nekoogar, "Digital Cryptography: Rijndael Encryption and AES Applications," October 11, 2001. <https://www.eetimes.com/document.asp?doc_id=1275908>, accessed 10/09/2017.

> will be safe from quantum computers for the time being. … To break current cryptosystems, quantum computers must have between 500 and 2,000 qubits… However, existing quantum computers that we know about only operate with less than 15 qubits at present, so there is no immediate worry.[50]

Thus far, Rijndael is living up to its promise as an adaptable and strong encryption algorithm.

The value of the NIST work was recognized by both Government and industry. In 2001, the AES team (Figure 2-6) received the Department of Commerce's Gold Medal Award for Leadership and the RSA Public Policy Award for significant contributions to the application of cryptographic technologies towards the advancement of personal privacy, civil justice, and basic human rights.[51]

***Figure 2-6. Department of Commerce AES Team Gold Medal Awardees***

From left (standing): Edward A. Roback, William E. Burr, Jim Nechvatal, Morris Dworkin, and Miles Smid. (Seated): Elaine Barker and James Foti. Not pictured are Jim Dray, Larry Bassham, and Juan Soto, 2001.[52]

### 2.4.5 Cryptographic Algorithm/Module Validation Program

NIST's work did not end in 2001. New computer technology and advancements require constant evaluation of AES modes and implementations. To provide assurance concerning AES and other cryptographic implementations, NIST sponsors the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP). These programs are the interface between NIST's

[50] http://www.technewsworld.com/story/84837.html, accessed September 27, 2017.

[51] *Information Technology Laboratory Technical Accomplishments 2001* (NISTIR 6815), NIST, November, 2001, p. 42.

[52] https://gcn.com/Articles/2001/06/28/NIST-goes-public-to-keep-Federal-secrets.aspx.

approved algorithms and the industries that implement them in products and services. The testing is done through pre-approved labs using NIST methodology, and passing implementations receive a FIPS-140 validation certificate which is published on the NIST CSD website.

FIPS-140-2 lays out the minimum requirements for cryptography considered suitable for Federal Government use. Federal agencies are required to use validated cryptographic modules and/or products containing validated modules, referred to as "being FIPS-140 compliant." NIST is clear that use of non-validated cryptography is viewed as "providing no protection to the information or data."[53] NIST established the programs in 1995 to provide testing and validation services for cryptographic implementations and modules to IT hardware and software manufacturers, integrators, and developers. Once validated, a module is eligible for use by Federal agencies.

The Cryptographic Algorithm Validation Program (CAVP) tests the encryption algorithms coding and mode of operation parameters. This test is brief and primarily involves encrypting and decrypting sets of data to ensure the submitted code functions as intended. The Cryptographic Module Validation Program (CMVP) is a more rigorous set of tests that provide validation concerning the hardware or software module that contains cryptography. The CMVP requirements cover design and implementation of the cryptographic algorithm, the physical environment and security, operational modes and environment, key management, electromagnetic compatibility, and ability to withstand attacks, among other things. "Module" is a broad term covering a wide variety of products. Modules range from a standalone hardware black box that sits between a computer's hard drive and external access and encrypts data that passes through it, to a software library file built into an operating system that provides encryption instructions and code for other programs to reference and use in their operations.

Cryptographic and Security Testing (CST) laboratories are authorized by NIST, through the National Voluntary Laboratory Accreditation Program (NVLAP), to perform CAVP

[53] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program, heading "Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments."

and CMVP testing. There are currently 21 CST labs, located internationally.[54] The CST laboratories perform CAVP and CMVP testing with validation tools developed by NIST and provided to the laboratories.

In the sixteen years from January 2002 through December 2017, there have been 2,521 CMVP certificates issued for modules with AES implementations. Of these, 1,034 are active certificates and 1,487 are historical or revoked certificates. No duplication exists between historical and active certificates in the CMVP database.[55] A certificate for a distinct module generally includes multiple encryption algorithms, meaning it can use all the listed algorithms or is interoperable with other systems that use them.

With the assistance of a few CST lab directors, certified modules listed on NIST's website were classified by major product type. Table 2-2 ranks all historical and active module certificates containing AES by major product type.

*Table 2-2. AES CMVP Certificates by Major Product Type*

| Module Type | Percent of Total AES Certifications | Number of Certifications |
|---|---|---|
| Network Appliance | 34.8% | 878 |
| Processor | 30.1% | 760 |
| Crypto Library | 11.1% | 279 |
| Storage | 7.6% | 192 |
| Authentication System | 4.8% | 122 |
| Radio | 3.5% | 88 |
| Toolkit | 3.3% | 82 |
| Key Management | 3.2% | 80 |
| Digital Cinema Projector | 1.6% | 40 |

Based on a careful reading of each certificate including AES, modules can be further classified into the hardware and software product subtypes, as described in Table 2-3.[56]

[54] https://www-s.nist.gov/niws/index.cfm?event=directory.results.

[55] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program.

[56] "Firmware," while a valid category, makes up less than 1% of CMVP certifications, and is therefore not included in this table.

*Table 2-3. CMVP Module Product Types and Subtypes*

| Module Type | Hardware Subtype | Software Subtype |
|---|---|---|
| Storage | Solid state, hard drives, tape drives, USB drives, and in-line storage encryption devices | N/A |
| Network Device | Routers, Switches, Mobility Controllers, Firewalls, Network Management Devices | Virtual Routers, Virtual Switches, Virtual Firewalls, Virtual Network Management Software |
| Cryptographic Library | N/A | Cryptographic Libraries |
| Toolkits | N/A | Cryptographic Toolkits contain software developer tools to assist in implementing encryption capability |
| Encryption Engines | Standalone encryption processor device (hardware security module) – frequently includes key management functions | Software based encryption processors use existing hardware CPU to perform encryption, and generally include key management functions |
| Key Management | Standalone key management device for generating, storing, and securely destroying keys | Software based Key Management program |
| Accelerators | Standalone encryption accelerator device – used to offload encryption in data centers and heavy traffic networks | Software based encryption acceleration program |
| Authentication System | Hardware components include ID cards, chips, and chip readers | Software modules include smart card applications, encryption processor programs, card/chip reader program |
| Other or Specialty Devices | Other hardware devices: Radios, Digital Cinema Projectors, Postal Meters, Printers and Telephones | Other encryption software: Radios |

# 3. Economic Analysis Framework

## 3.1 FIPS in Economic Context

This section provides a brief introduction to the economic significance of FIPS: the switching costs that a new FIPS entails; FIPS as public goods; as market-failure mitigating tools; and as infra-technology. The discussion provides some context for understanding the purpose of survey questions posed to respondents, the survey results, and the economic impact calculations.

### 3.1.1 Encryption Systems and Switching Costs

An information *system* enables information to be stored, searched, retrieved, copied, filtered, manipulated, transmitted, received, and secured. Information systems typically consist of multiple pieces of hardware and software that require specialized training and that must be integrated to function effectively.[57] The "networked" nature of the information system has implications for its value to users: the value of connecting depends on the number of other users already connected to it.[58] This is true of railroad networks, ATM networks, email networks, and even fire hydrant networks—an example that will be taken up in Section 3.1.5 ("FIPS as Infra-technology").

An industry rule of thumb, referred to as "Metcalf's Law," holds that if there are *n* people in a network, the value of the network to each of them is proportional to the number of other users, and the total value of the network (to all the users) is proportional to $n \times (n-1)$ or $n^2$-$n$. Accordingly, if the value of the network to a single user is $1 for each other user on the network, then a network of size 10 has a total value of approximately $100, and if the size of the network is 100, the approximate total value is $10,000, a 100-fold increase in the network's value to all users for only a 10-fold increase in network size.[59]

New technologies that are incompatible with popular networks, or users considering a change of networks, must overcome the costs of switching from one implementation of a technology to another, i.e., "switching costs." That can be a high hurdle. Switching costs

[57] Gregory Tassey "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, p. 223.
[58] Shapiro and Varian, op. cit., p. 174.
[59] Ibid., p. 184.

include all the costs required to move from one system to another. In the case of encryption, switching costs might include the cost of new hardware, new software, additional staff, or additional training. For providers of the new incompatible network technology, for example an encryption system based on AES rather than DES or TDES, it means overcoming the combined switching costs to users of the rival network, a factor working to the distinct advantage of incumbents.[60] In other words, collective switching costs encourage *lock-in* from both the users' and the providers' perspectives, a phenomenon also known as the "installed base effect."[61] Lock-in tends to be durable because specialized databases—the information that information systems store, search, retrieve, copy, filter, manipulate, transmit, receive, and secure—grow over time and thereby, all else remaining equal, increase the costs of transitioning to alternative networks.[62] Of course, lock-in can be overcome by new service providers, but it relies on delivering value in excess of total switching costs.[63]

In relation to encryption, different algorithms require different hardware and software implementations to operate effectively. DES and TDES were the most commonly used symmetric block algorithms prior to AES.[64] Switching costs to move from DES/TDES to AES could include the costs of new hardware, new software, software updates, new training, and migrating stored data to the new algorithm (decrypting and re-encrypting stored data). Appendix A contains a historical case study of encryption system switching costs involved in the transition from DES to TDES to AES in the banking and finance sector.

### 3.1.2 Interoperability, Compatibility, and Standardization

Two communication networks lack interoperability if subscribers on one network cannot communicate with those on the other network. Two hardware/software systems are incompatible if the components of one system do not work with components of the other system.[65] Encryption system costs rise when more than one encryption "language," or algorithm, is used to communicate with all the computers in the network: longer

[60] Ibid., p. 184.
[61] Ibid., pp. 133-134.
[62] Ibid., pp. 122-123.
[63] Ibid., p. 111-15.
[64] This statement is specifically about symmetric block ciphers.
[65] <http://www.testingstandards.co.uk/interop_et_al.htm>.

processing time requires more power; transmitting data may be slower; maintenance and repair may be more complex. As more computers use the same language, costs decrease and ease of use increases.

Standardization expands the benefits of networks by enhancing interoperability and compatibility, making it possible for one network to share information with a larger network, thereby attracting more consumers. Standards play a large role where information technology is ascendant. Shapiro and Varian claim that formal standard-setting processes have never been more important to market competition.[66] In addition to enhancing network externalities, standards tend to reduce risk to consumers by bolstering the credibility of technology, reducing consumer lock-in if standards are open, shifting the locus of competition from competing for market dominance to competing for market shares, as well as shifting the nature of competition from systems to components and from features-competition to price-competition.[67]

### 3.1.3 Standards as Public Goods

"Public goods" are goods and services that benefit all consumers but that tend to be undersupplied by private sector investors because they are "nonrival" *and* "nonexcludable." A good or service is nonrival if the marginal cost of providing it to an additional consumer is zero, that is, if consumption of the good or service by one consumer does not diminish its availability for other consumers.[68] A good or service is nonexcludable if people cannot be excluded from consuming it. The classic example of a pure public good is national defense. Once it is provided, all citizens enjoy it. The transparent and international process by which FIPS-197 was developed, selected, and made freely available to the public is similar to national defense in this regard. The AES is both a nonrival and nonexcludable public good.[69]

[66] Shapiro and Varian, op. cit., p. 237.

[67] Ibid., p. 228.

[68] Classic examples of nonrival goods are highways (during low traffic volume) and lighthouses. Since the highway and the lighthouse already exist, the marginal cost of providing these services to additional consumers (drivers in the first instance, ship pilots in the second instance) is zero.

[69] As a practical matter, it is more common to find goods and services that have one "public good" characteristic but not the other so that the "publicness" of public goods is best considered as falling on a spectrum of publicness, ranging from pure public goods (national defense) to pure private commodities. Even industry-driven consensus standards developed and published in the United States by standards development organizations (SDOs) may not be *pure* public goods to the extent that access to them comes at cost that could effectively exclude some potential users. In any event, SDOs produce standards with

While public goods and services are provided by public and private institutions, it is likely that the government will play an important role in providing them at a level commensurate with societal welfare. The publicness characteristics of public goods make the role of public institutions (or other forms of collective action, such as standards consortia) instrumentally important. Private for-profit organizations invest to generate a return on their investment in excess of opportunity costs. If these returns cannot be realized, it makes little sense to make the investment. Public organizations, on the other hand, can take a broader view. If they can demonstrate a broad benefit to society of an investment in public goods and services, that investment (on the part of the public) may be justifiable because the total benefits (summed across all beneficiaries) may exceed the social cost by a sufficient amount to justify the public investment.[70]

The know-how and services provided by NIST's CSD—such as FIPS-197 and FIPS-140-2, as well as a library of "Special Publications" concerned with modes of operation and various aspects of computer security assessment—are public goods in the sense just described. NIST's AES program has provided cryptographic infrastructure technology (that arguably would be underprovided by the private sector acting alone) to improve the economic performance of cryptographic goods and services.

### 3.1.4 FIPS as Market Failure-Mitigating Tools

When the buyers in markets realize the benefits of their purchases, and the suppliers face the costs of the resources that they use for production, if markets have an adequate number of buyers and sellers engaged in a competitive process, the signals provided by market prices to the market's participants are generally believed to enable the market mechanism to allocate scarce resources efficiently. Market failures are instances where prices do not adequately reflect the value of resources and consequently resources are not

considerable public goods content. On the imagined spectrum of publicness, FIPS-197 is located closer to the pure public goods end of the spectrum than FIPS-140-2. To the extent that fees are paid to obtain certification, FIPS-140-2 would appear to be somewhat less non-excludable than FIPS-197. However, modes of operation specifications *are* freely available, even if a certificate is not. FIPS-140-2 is closer to a pure public good on the spectrum of publicness than would be if the specifications were not freely available.

[70] From an economic perspective, there is a threshold return on an investment established by the cost of public borrowing. The cost of public borrowing is addressed in Office of Management and Budget Circular A-94. See Albert Link and John Scott, *Public Accountability: Evaluating Technology-Based Institutions,* Kluwer Academic Publishers, 1998, pp. 17-21.

efficiently allocated. Instead, too many of society's resources are used in some activities, while too few are used in others.

In the context of investments in new technologies, there are many types of barriers to technology development and commercialization that can cause too few resources to be allocated to those activities, leading to underinvestment by the private sector. Some of the underinvestment is routinely mitigated by government programs and/or collaborations with industry and university partners.[71] Generally speaking, these barriers to technology development cause risk and uncertainty to rise and reduce the ability of private firms to capture sufficient investment returns to justify the private investments in socially valuable technology. If such barriers are not mitigated they can lead to market failures by underinvestment in socially valuable technology.[72] If the various barriers to technology development and commercialization are reduced, allowing private firms to realize higher returns and lower risk on their investments, private investment more closely approaches its social value. Thus, government initiatives that reduce barriers to technology development, and thus stimulate a socially desirable level of investment, function as market failure mitigating policy tools. FIPS are an example of market failure mitigating policy tools.

Barriers to cryptographic technology development and commercialization were quite high when NIST's AES program was initially launched in the mid-1990s. According to a contemporaneous 1996 National Research Council report, the United States was "in the midst of a policy crisis, unable to develop a consensus about cryptography policy."[73] The dimensions of the crisis included the following:

[71] Tassey, *Economics of R&D,* op. cit., especially Chapter 5, "Rationales for Public Sector R&D Policies," and Chapter 6, "Alternative Policy Mechanisms," pp. 81-130.

[72] The following categories of technology development and commercialization barriers have been identified as precipitating market failures: externalities, information-sharing difficulties, recognition, long time to market, incompatibility, and inadequate infra-technology. For a fuller discussion, with additional examples, see, David Leech, Albert Link, and John Scott, *The Economics of a Technology-Based Service Sector,* NIST Planning Report, No. 98-2, U.S. Department of Commerce, January 1998, especially pp. 27-36; Gregory Tassey, *The Economics of R&D Policy,* Quorum Books, 1997 (especially Chapter 5, "Rationales for Public Sector R&D Policies," pp. 82-100). For a discussion of the "market failure" modes that these barriers may precipitate, see John Roberts, *The Modern Firm,* Oxford University Press, 2004; and Oliver Williamson, *The Economic Institutions of Capitalism,* Free Press, 1985.

[73] *Cryptography's Role in Securing the Information Society*, National Research Council, 1996, p. xvi.

1. Export restrictions reduced the private sector incentive to invest in R&D for a new algorithm.
2. Industry could not agree on what stronger encryption looked like, and what was actually possible to achieve.
3. There was lack of demand for stronger encryption in the broader market and uncertainty about future demand. (In the mid-1990s, only a minority of technical experts and cryptographers understood the growing need for information security in the Internet-based society that was in its infancy.)
4. The cost of cryptographic products was high. (Prior to AES development, much of encryption was performed by separate standalone chips and hardware boxes. The cost of incorporating encryption hardware was higher than today, where encryption is often performed from a set of program files.)
5. Lack of certification/verification/validation of encryption implementations stronger than DES or TDES led to consumer uncertainty about the value and actual performance of encryption.
6. Lack of interoperability between different computer systems and software, and lack of encryption standards to bring industry together, was leading to a fragmented-market situation with "everyone rolling their own" encryption protocols.
7. Industry and consumer distrust occurred because of concerns that encryption standards from the government were designed with a capability for the government to access private communications. As a result, many computer and automated systems lacked encryption protections.[74]

While all of the above would have contributed to commercial uncertainty, the technical uncertainty associated with cryptography has always been high. In the words of a current cryptographer, it is "fiendishly difficult" to develop an encryption algorithm, so much so that, "even seasoned experts design systems that are broken a few years later."[75] The situation around 1995 seemed set up for market failure where encryption technology was concerned. The development of the FIPS-197 on a not-for-profit, open, royalty free basis

[74] Ibid.

[75] Ferguson, op. cit., p. 13.

pulled the market away from this impasse and supported the following decades' tremendous growth of computer and internet products and services.

### 3.1.5 FIPS as Infra-technology

NIST's role in the economy has been conceptualized as providing "infrastructure technology," or "infra-technology." Just as roads and bridges are frequently referred to as the infrastructure of regional and national economies—because they reduce the cost of getting from here to there and, thereby, expand the geographic boundaries of markets for goods and services—infra-technology serves a similar function in the realm of R&D processes, product development, and product commercialization.[76]

AES and the CAVP and CMVP—FIPS-197 and FIPS-140-2—are quintessential infra-technologies. The process by which AES was developed is a textbook case of government-industry cooperative investment and has been touted as a shining example for developing similar standards.[77] FIPS-197 can be understood as a cryptographic *product standard* (inasmuch as source code is a product): a set of specifications to which some or all elements of products under its jurisdiction must conform. In the same way, FIPS-140-2 can be understood as a cryptographic *non-product standard*. Together they represent public goods of significant economic value that likely would not have been forthcoming from the private sector alone. As explained in Section 3.1.4, risk and uncertainty associated with the networked nature of encryption system, the high public goods content of effective encryption algorithms, the sheer technical difficulty of designing sufficiently strong algorithms, and the uncertainty surrounding the international market for encryption products would have reduced the ability of private firms, acting alone, to capture sufficient investment returns to justify the private investments in socially valuable technology on par with what NIST provided.

[76] The term "infra-technology" was coined to describe the "technical tools" that are ubiquitous in a high-tech economy and provide substantive foundation for many standards. Infra-technologies include measurement and test methods, standard artifacts (such as standard references materials or weights and measures artifacts), scientific and engineering reference databases, process models, and the technical basis for both physical and functional interfaces between the components of systems technologies. See, Gregory Tassey, *The Economics of R&D Policy,* Quorum Books, 1997.
[77] Ferguson, et. al., op. cit., p. 321: "AES is the shining example of how to standardize security systems."

As infra-technological product and non-product standards, FIPS-197 and FIPS-140-2 had the potential to significantly reduce costs across the three major stages of technology-based economic activity: R&D, production, and commercialization.[78] They exhibit three of the four functions typical of standards in knowledge-intensive industries:

(1) Enable variety reduction among designs and functions of product elements (FIPS-197);

(2) Specify quality and reliability of product and process technologies (FIPS-140-2); and

(3) Provide performance-related information on characteristics of resources and actual products and processes (FIPS-140-2).[79]

These functions, operating across the stages of product development and commercialization, are largely responsible for creating the cost avoidance benefits and economic impacts described and estimated in the following chapters of this report.

## 3.2 Encryption Systems in an Industrial Context

### 3.2.1 Encryption Systems Value Chain

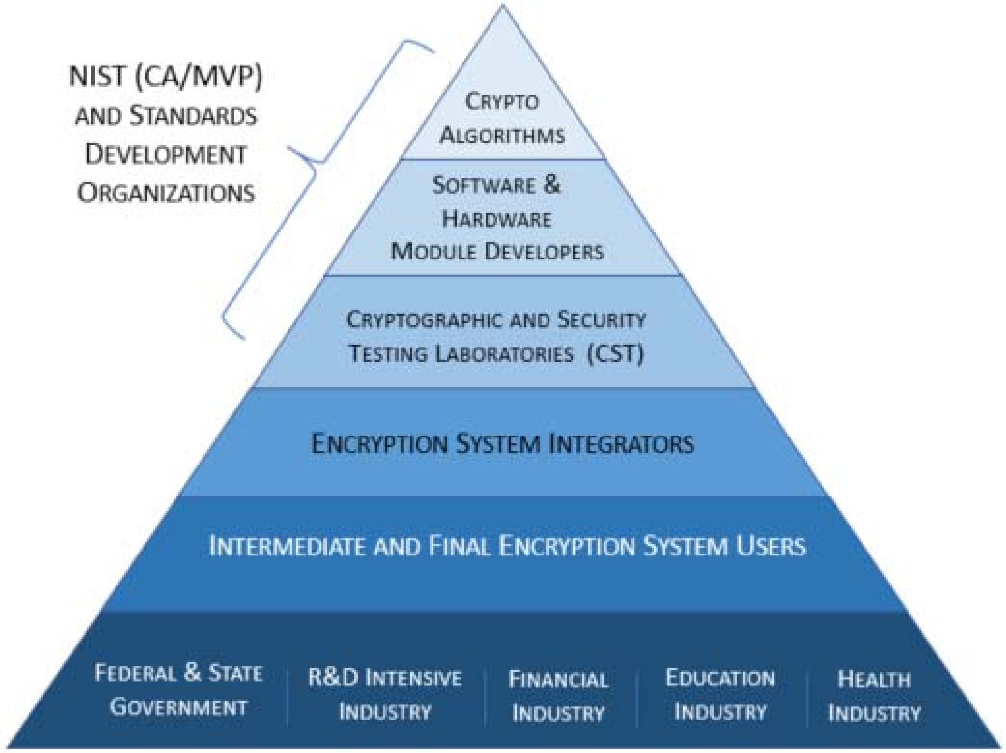
The value chain depicted in Figure 3-1 is a snapshot of the complex process by which many economic actors contribute their ingredients to product and service integrators further down the chain and, ultimately, to intermediate and final users of encryption services. Value chains are conventionally thought of in terms of the upstream sources of basic technology (cryptographic algorithms) and the value added as they move downstream through the tiers of the value chain toward intermediate and final users.[80]

[78] Ibid., p. 247.

[79] Ibid., p. 228. Tassey defines the fourth function to be the assurance of interoperability for hardware and software components of technology-based systems. Neither FIPS-197 nor FIPS-140-2 assure interoperability of two or more encryption systems except to the extent that the systems, independent of the certification process, employ AES-certified hardware and software modules. FIPS-140-2 certification does not certify the encryptions systems that utilize certified modules.

[80] It has become commonplace to discuss information-intensive and networked industries in terms of an "ecosystem" of which they understand themselves to be a part. See, for example, M. Iansiti and R. Levien, *The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovations, and Sustainability,* Harvard Business School Press, 2004; and David Evans, et. al., *Invisible Engines: How Software Platforms Drive Innovation and Transform Industries*, MIT Press, 2008. However, knowledgeable industry representatives assert that cryptographic software and hardware developers and integrators *do not* tend to use the language of ecosystems to describe the dynamics of their industry, so the more conventional description of a vertical value chain is used here.

*Figure 3-1. The Encryption System Value Chain*


NIST (CA/MVP) and Standards Development Organizations
Crypto Algorithms
Software & Hardware Module Developers
Cryptographic and Security Testing Laboratories (CST)
Encryption System Integrators
Intermediate and Final Encryption System Users
Federal & State Government
R&D Intensive Industry
Financial Industry
Education Industry
Health Industry

***Cryptographic algorithm developers*** are specially trained or experienced mathematicians. The Bureau of Labor statistics reports 40,300 employed mathematicians in 2016.[81] Only a very small fraction of these was likely employed in the development of cryptographic algorithms. Reportedly, most cryptographers work for the NSA, other government agencies, or in academia. Commercial cryptographers are likely few in number and probably primarily employed by large multi-national corporations.[82]

***Cryptographic module developers*** are surely the employers of some cryptographic algorithm developers. The only systematic source of information concerning module developers is NIST's CMVP, which allows for commercial companies to submit encryption products for formal testing by CST labs. If approved, the product becomes eligible for sale to the Federal Government. As of December 2017, the companies holding the largest number of active *AES hardware validation* certificates included Cisco Systems, Thales e-Security, Motorola Solutions, SafeNet, and Brocade Communications

[81] https://www.bls.gov/ooh/math/mathematicians-and-statisticians.htm.
[82] https://www.bls.gov/careeroutlook/2012/fall/art01.pdf.

Systems. Companies holding the largest number of active *AES software validation* certificates included Microsoft, Apple, RSA, Red Hat, and Cisco Systems.

***Cryptographic and Security Testing (CST) laboratories*** are authorized by NIST, through the NVLAP to perform the CAVP and CMVP testing. There are currently 21 CST labs, including several international locations.[83] For most labs, such testing is 5% or less of their annual revenues.[84] Certificates are generally good for five years before re-evaluation is necessary. Industry participants estimated the average cost to obtain a CMVP certificate generally ranges from $50,000 to $100,000. This cost includes the testing lab fees, NIST cost recovery fees, internal testing, application preparation, and often consulting fees.

***Encryption system integrators*** incorporate validated modules into larger computer, computer peripheral, network equipment, and software systems. By and large they are thought to be the same companies that apply for cryptographic hardware and software module validations, but it is the modules alone, not the higher order equipment and systems, that are validated and certified. For example, the Microsoft Windows operating system contains a cryptographic module library with reference code for numerous encryption algorithms. It is this library file and the modes of access to it within the software that is submitted for CMVP testing, not the overall operating system product.

***Intermediate and final encryption system users*** represent a wide, and possibly widening, swath of industries. It is generally believed that Federal and state agencies, banking and finance, and health-related industries have been the heaviest users of encryption systems in the past. Federal agencies must secure confidential data with AES or TDES. A canvas of state agency Information Security Offices found that most are FIPS-140-2 compliant for at least some of their departments. Survey responses were received from across the economic landscape, beyond those historically identified with encryption, including: agriculture; construction; manufacturing; retail trade; transportation and warehousing; information; real estate rental and leasing; professional, scientific, and technical services;

[83] https://www-s.nist.gov/niws/index.cfm?event=directory.results.
[84] Estimate based on email exchanges with testing lab representatives.

management services; waste management; educational services; and arts and entertainment.[85]

***NIST and Standards Organizations*** interact with several layers of the value chain. NIST provides direction for the CAVP and CMVP. These two programs aid private sector companies in selling regulatory compliant products to the Federal Government. Passing modules receive a certificate of FIPS compliance and are listed on NIST's website allowing Federal entities to consult the list for FIPS compliant IT products.

Standards bodies dealing with encryption matters include the International Standards Organization (ISO), the Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), and the American National Standards Institute (ANSI). Since the issuance of FIPS-197, numerous standards have been revised or developed which reference FIPS-197 as a "normative reference," that is, *indispensable* to the application of the standard.[86] The strongest concentration of normative references occurs between 2008 and 2010, when numerous standards were issued concerning telecommunications and networking security, road vehicle security, digital cinema data security, and home security. These are indicative of the widespread introduction of digital platforms across the world at the end of the first decade of the 2000s. Touchscreen application-enabled phones were released, the concept of Internet of Things emerged, and "big data" and data driven analytics were becoming popular.[87] The first

[85] A dimension of the value chain that is not clearly depicted here includes products that are not "encryption systems" as we have defined them but which incorporate security algorithms or subsystems, for example, road vehicle security systems and digital cinema security systems. Encryption technology likely plays a role in any use scenario involving securing data from hacking or other threats. All such "every-day" examples of encryption applications fall into the "final encryption system user" tier.

[86] Standards referencing AES issued between 2008 and 2010 include: ISO/IEC ISO/IEC 26430-3: Digital cinema (D-cinema) operations—Part 3: Generic extra-theater message format; ISO/TS 24534-5: Automatic Vehicle and Equipment Identification; ISO/IEC 24767-2: Home network security, communication protocol for middleware; ISO/IEC 19772: Information technology—Security techniques—Authenticated encryption; ISO/IEC 18033-4: Information technology—Security techniques—Encryption algorithms—Part 4: Stream ciphers; ISO/IEC 24771: MAC/PHY standard for ad hoc wireless network to support QoS in an industrial work environment; ISO/IEC 11889: Trusted Platform Modules; ISO/IEC 18013-3: Information technology—Personal identification—ISO-compliant driving license; ISO/IEC 14543-5-1: Information technology—Home electronic system (HES) architecture; ISO/IEC 13141: Electronic fee collection—Localization augmentation communication for autonomous systems; ISO/IEC 13157-2: Information technology—Telecommunications and information exchange between systems—NFC Security—Part 2: NFC-SEC cryptography standard using ECDH and AES.

[87]The iPhone was first released in 2007.

digital camera filmed movies won Oscars.[88] Broadband Internet brought lightning fast banking, chat, shopping, and gaming to many American homes. Since 2011, the majority of encryption standards have focused on telecommunication networks. As the technology for fast Internet improves, the need to maintain equally fast and secure capabilities is paramount.[89] Banking and financial markets, doctor visits and health data, proprietary intellectual property and private information, car and phone navigation systems, shopping purchases and browsing habits, gaming and chat sessions—all rely on the Internet to some extent and involve data that people and companies wish to protect from unauthorized access and use.

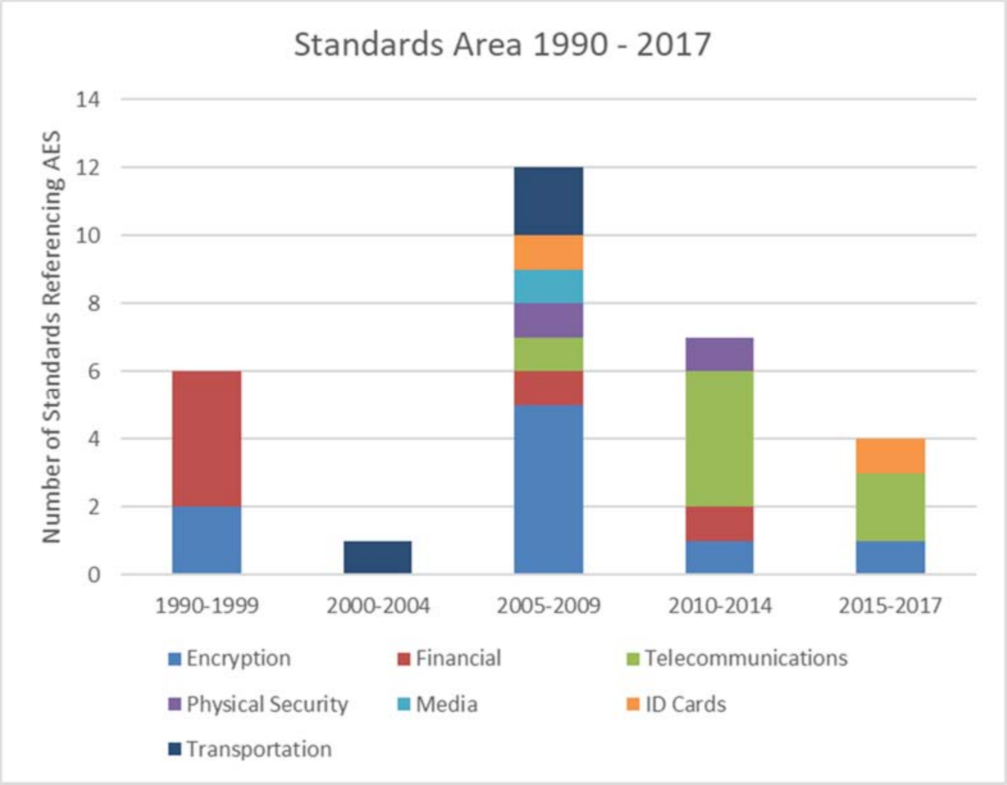
Figure 3-2 tracks the industries covered by AES-dependent standards over the years, that is standards containing a normative reference to AES, FIPS-197. In the Figure, the year is based on first year the dependent standard was released.[90] Many financial industry related standards were released pre-AES and were subsequently revised in years following the 2001 publication of FIPS-197. The chart captures the general development in AES-dependent standards over time. Developing a new standard generally takes two to five years; thus, the period of 2000 to 2004, immediately after the release of FIPS-197, sees only one AES-dependent standard in transportation issued, while the subsequent period from 2005 to 2009 has the largest concentration of new AES-dependent standards. It is probable that a majority of the standards issued in the 2005 to 2009 period were under development in the preceding period from 2002 onward.

[88] *Slumdog Millionaire* was the first all-digital film to win an Oscar in 2009.

[89] Seven additional AES related ISO standards were identified between 2011 and 2017, four of which are related to telecommunications or streaming protocols. They include: ISO/IEC 16504:2011—Information technology—Telecommunications and information exchange between systems; ISO/IEC 23001-7:2015: Information technology—MPEG systems technologies; ISO/IEC DIS 23009-4:2013: Information technology—Dynamic adaptive streaming over HTTP (DASH); ISO/IEC 13157-3:2016: Information technology—Telecommunications and information exchange between systems.

[90] In many cases we could only ascertain the initial year released and the most recent revision. Thus, we could not precisely determine when the post-AES standard revision was released in most cases.

*Figure 3-2. AES-Dependent Standards*



### 3.2.2 Encryption System Market Size and Composition

In 1986, a Congressional Office of Technology Assessment study reporting on what it called the "Government Information Revolution" provided that, "despite the fairly widespread agency use of electronic dissemination of [Federal] Government information, such use is still largely in the formative stages."[91] By 1991, the National Academy of Sciences, worrying about the risk posed to data confidentiality, concluded:

> Whereas the market in 1980 was dominated by commercial computer and communications systems with *no security features*, the market in 1990 includes a significant number of systems that offer discretionary access control and a growing number from both major and niche vendors with both discretionary and mandatory access control, which provides significant protections against breaches of confidentiality. (Italics added.)[92]

[91] *Federal Government Information Technology: Management, Security, and Congressional Oversight*, Congress of the United States, Office of Technology Assessment, February 1986, p. 145.

[92] *Computers at Risk,* National Academy of Sciences, 1991, p. 143.

Attempting to characterize more precisely the size and shape of the market for cryptography, the authors of an influential report by the National Research Council (1996) found what this report's investigation of the market for encryption systems found:

> The committee was unable to determine the size of the information technology market directly affected by export controls on encryption... the floor of such estimates—a few hundred million dollars per year—is not a trivial sum. Furthermore, all trends point to growth in this number, growth that may well be very large and nonlinear in the near future. ...Most sales of information technology products with encryption capabilities are integrated products.... the market for cryptography is... not well defined when integrated products with encryption capabilities are involved.[93]

The situation today is similar. Respected market analysts can clearly identify market segments of software and network equipment and estimate their market value and share distribution, but they are unable to estimate the security-related portions. What market size and share distribution information is readily available is of questionable veracity and cannot be ascertained without purchasing the questionable data.[94] The companies identified as the predominant market participants in the readily available estimates of encryption-related software and hardware markets are among those identified as the top five CMVP certificate holders (listed in the discussion earlier of cryptographic module developers).

This chapter developed an economic analysis framework by placing the AES program in its broader economic and industry context. From an economic perspective, high and rising switching costs and the subsequent lock-in effect of networked systems can act as barriers to the development and adoption of more efficient and secure encryption systems. This chapter explained that standardization, generally, is a method of reducing the costs associated with the lack of network interoperability and incompatibility. It

[93] *Cryptography's Role in Securing the Information Society,* National Research Council, 1996, pp. 148-49.

[94] This is a problem referred to as "the information paradox" whereby the value for the purchaser is not known until the information is reviewed, and the provider is unwilling to allow review prior to purchase. Kenneth Arrow, "Economic Welfare and the Allocation of Resources for Invention," p. 615, in *The Rate and Direction of Inventive Activity: Economic and Social Factors*, National Bureau of Economic Research, Princeton University Press, 1962.

discussed how the public goods nature of standards causes them to function as tools for mitigating technology development barriers that lead to market failures.  FIPS-197 and FIPS-140-2 were further characterized as infra-technological standards with the potential to generate significant cost-avoidance benefits.  Finally, this chapter introduced the encryption system value chain, from cryptography developer to intermediate and final users of encryption systems.

Chapter 4 will build on the economic and industry analysis framework to identify specific cost-avoidance benefits enabled by the AES program, map out a plausible counterfactual scenario, and identify the categories of potential beneficiaries.

# 4. Economic Impact Assessment Approach

## 4.1 Survey Strategy

The central question posed by the survey for this economic impact assessment was, "What would it have cost industry, acting without NIST support, to develop and adopt a strong successor to the operative encryption standard (DES, FIPS-46) in the mid-1990s as DES was coming to the end of its useful life as a secure symmetric block cipher?"[95]

The answer to the basic question requires answers to the following questions:

> Would the private sector, acting alone, have developed a standardized strong and efficient replacement for DES sooner or later than the year 2000 (the year the *Rijndael* cryptographic algorithm was selected as the AES)? If not, why not?
>
> If the private sector would not have developed a standardized strong and efficient replacement for DES sooner than 2000, what would have been the consequences? In other words, what kinds of costs and risks would have been incurred by developers and users of encryption systems in the absence of a widely accepted replacement for DES in 2000, and for how long would those costs have been incurred?
>
> What jargon or technical terms and units of measure are used by the community of cryptography developers and users to describe and discuss the costs and risks associated with relatively weak encryption?

These and derivative questions were posed by the authors in their reading of published literature concerning the AES, and in interviews and email exchanges with members of NIST's original AES competition program team and several experienced industry representatives and cryptographers. Some of the latter had developed algorithms for the AES 1997 competition. These scoping interviews attempted to clarify the timeline for the study, establish important stages in the AES program and their dates, ascertain

[95] This question entails what is described as the "counterfactual method," the appropriate method for assessing the economic impacts of publicly funded, publicly performed investments. See, Albert Link and John Scott, *Public Goods, Public Gains: Calculating the Social Benefits of Public R&D,* Oxford University Press, 2011, pp. 31-32.

possible motivations for the program and the problems it addressed, and to differentiate the many areas of economic benefits (cost avoidance) practitioners hoped to achieve.

In parallel, a plausible counterfactual scenario of what might have happened in the absence of NIST was developed. This further clarified the nature of various cost avoidance benefits enabled by the AES program. Characterization of cost avoidance benefits and the counterfactual scenario provided a framework for developing hypotheses about the broader economic impact of AES, and finally, survey questions.

### 4.1.1 Seven Broad Categories of Cost-Avoidance Benefits Identified

The retrospective impact of NIST's AES program is primarily the function of the costs avoided by having a central, trusted body take the initiative and bear some of the costs of the development of a stronger, computationally more efficient and flexible replacement of DES and the interim TDES.

In the absence of NIST's leadership, the evolution of a sufficiently strong and efficient encryption technology and its implementation as AES would have been significantly retarded. From the supply side of the market, the costs of related R&D, production, and commercialization would have been higher.[96]

The survey questions were designed to help quantify several categories of potential avoided costs identified in scoping interviews and historical research conducted by the authors. Large-scale encryption systems such as in-house data centers and cloud computing services were the organizational focus of the survey directed at encryption system consumers. Multiple servers and communication equipment are typically co-located in data centers due to their environmental requirements, ease of maintenance, and physical security needs. It was assumed that management personnel associated with data centers or reporting to Chief Information Security Officers (CISOs) would have ready access to information concerning the performance and costs associated with encryption systems.[97] Senior technical managers were the focus of survey questions directed at cryptographic module developers and encryption system integrators.

[96] Ibid.

[97] Personal communication with data center industry analysts, Peter Christy (12-5-17 through 3-13-18) and Andy Lawrence (12-6-17 through 12-8-17). See, also, *A Peep Into Data Center Economics: Analyzing*

Survey questions were developed to obtain estimates concerning hypothesized areas of avoided costs including the following:

### 1. Avoided costs of slower processing speed

A test of encryption speeds between TDES and AES determined that AES was approximately six times faster than TDES on current hardware. It was assumed that, all else held constant, slower processing speeds would require additional resources. The survey questions asked respondents to quantify the additional resources.

### 2. Interoperability costs avoided

To tackle interoperability costs, it was assumed that in the absence of AES, developers and integrators would have to duplicate efforts writing code and performing maintenance on multiple algorithms. It was hypothesized that without AES, there would have been a fragmented market with multiple algorithms in use within or across different industrial sectors. These benefits would accrue to consumers and producers of encryption systems, and respondents were asked to quantify such benefits.

### 3. Breach costs avoided

Between 1996 and 2016, there was no indication that AES was successfully attacked and broken by brute force attacks or cryptanalysis. DES, on the other hand, was susceptible to attack, and by association TDES was susceptible, too. It follows that organizations moving to AES would receive intangible benefits by reducing the likelihood of successful cryptanalysis attacks. Moreover, absent AES, there would have been more diversity among the strong encryption algorithms in use by networks both during and after the time of the AES competition and the selection of the new standard. Such multiplicity of algorithms would have caused additional complexity and potential lapses enabling hackers to breach security systems. In the survey questions, encryption system users were asked to disclose the average annual number of cyberattacks against encrypted data over the past five years, as well as describe their understanding of the relationship

*Challenges & Opportunities,* Wipro Technologies, 2011; and Luiz Andre Barroso, Jimmy Clidaras, and Urs Holzle, *The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines,* Second Edition, 2013 (1st edition, 2009), Google, Inc.

between multiple encryption algorithms, resulting interoperability issues, and the risk of successful breaches.

### 4. Pre-acquisition costs avoided

In the face of fragmented markets, the resulting interoperability issues and an absence of consensus standards, organizations purchasing encryption systems would be forced to engage in a host of pre-acquisition activities that raise costs. These activities typically include product search costs, qualification-testing costs, and acceptance costs. Survey respondents were asked to estimate any increases in these and related costs in the counterfactual absence of AES.

### 5. Standards development costs avoided

There are multiple industry organizations that develop encryption standards including the ISO, IEEE, IETF, and ANSI. These organizations rely on volunteered time from experts working in industry and government. Since NIST took on the task of evaluating algorithms and producing a standard, the standards organizations and commercial entities received a benefit of reduced costs for standards development. Currently, these standards organizations have issued guidance that reference FIPS-197 and FIPS-140-2. In the absence of NIST's work, it was hypothesized these organizations would have incurred more labor hours and longer delays to produce standards and guidance in this area. Survey respondents were asked for estimates of these hypothesized effects on their organizations.

### 6. Lost sales and profits avoided

Over and above the costs avoided in the development of AES-dependent standards, sales of standardized products and services would also have been affected. Survey respondents were asked to estimate how market growth would have been affected absent AES.

### 7. Hardware and software module quality degradation avoided

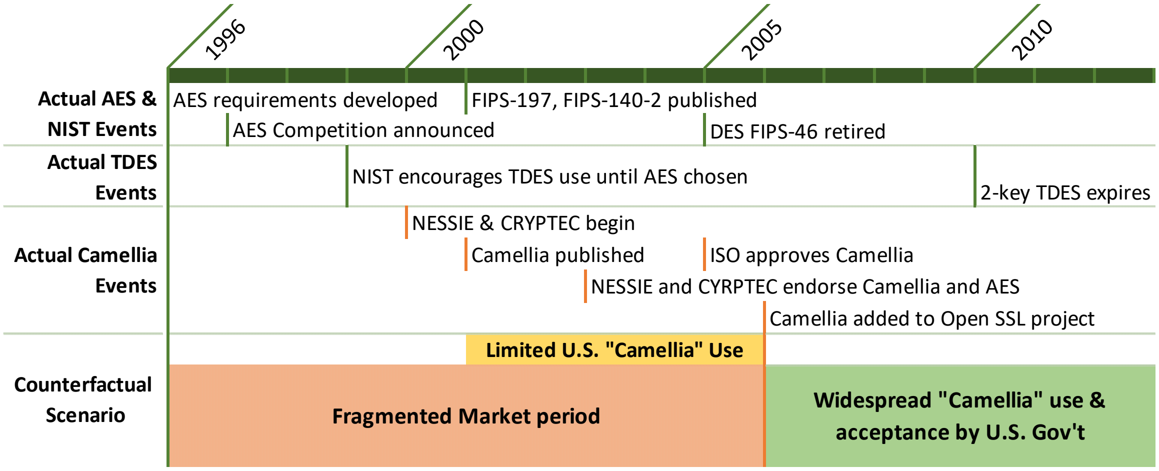
The validation process associated with FIPS-140-2 compliance adds value to cryptographic modules and systems. In the absence of the AES program, both the avoided costs for producers to assure the quality of their products and the added confidence afforded consumers of encryption systems would have been foregone. Survey respondents were asked to estimate these benefits.

### 4.1.2 The Counterfactual Scenario

The counterfactual scenario is used as a means for pulling background research and interview information together and conceptualizing the economic benefits of the AES program by imagining what would have happened had it been postponed or had never occurred. A time series of the estimated annual sum of costs avoided is interpreted as the economic benefits of the AES program, and those benefits are then compared with the program's actual costs.

Figure 4-1 graphically depicts some main events of the AES program (top panel). The period under investigation begins in 1996, the year NIST's CSD began to organize internally for the AES competition the following year. Without NIST, what would have happened from this point on?

*Figure 4-1. AES program Timeline & Counterfactual Scenario*


1996
2000
2005
2010
Actual AES & NIST Events
AES requirements developed
FIPS-197, FIPS-140-2 published
AES Competition announced
DES FIPS-46 retired
Actual TDES Events
NIST encourages TDES use until AES chosen
2-key TDES expires
Actual Camellia Events
NESSIE & CRYPTEC begin
Camellia published
ISO approves Camellia
NESSIE and CYRPTEC endorse Camellia and AES
Camellia added to Open SSL project
Counterfactual Scenario
Limited U.S. "Camellia" Use
Fragmented Market period
Widespread "Camellia" use & acceptance by U.S. Gov't

Camellia, a modern algorithm with technical similarities to AES (third panel), was released in 2000 and endorsed by the ISO in 2005.[98] Camellia's development timeline synchronized well with industry estimates of standards development times.

[98] Camellia is a 128-bit symmetric block cipher very similar in operation to AES. It was developed jointly by the Japanese companies Mitsubishi Electric and Nippon Telegraph and Telephone (NTT) and released in 2000. In 2005, the ISO/IEC accepted it as an encryption standard. It was endorsed by the European NESSIE and Japanese CRYPTEC committees as a recommended cipher alongside AES. Some U.S. technology experts suggested that Camellia was developed as a Japanese national version of AES and suggest that Camellia would not have existed without the NIST competition and the resulting AES.

Due to the infra-technological nature of the AES program, the benefits of the AES program were expected to span the product life cycle of cryptographic products and services, from R&D to commercialization.[99] The "absent NIST" counterfactual (bottom panel) has three components: market fragmentation, consensus standardization in the absence of AES, and the TDES option. It was hypothesized that market fragmentation would have ensued from 1997 to 2004 while industry and standards organizations sought a strong unified alternative to DES and TDES.

The hypothesized market fragmentation which industry representatives described in the 1990s would have extended through approximately 2005. This period would have had multiple, post-TDES strong and efficient solutions emerging.[100] Minimally five, possibly more, of the original 15 algorithms submitted to the AES competition could have been pursued even though it is known, as a result of the analysis performed during the AES competition, that some of the 15 had serious flaws and would not have been successfully developed. These solutions would have emerged in response to an increased need for security driven by increasing risk of attacks and security breaches, as well as in response to Federal, state, and international regulations passed since 1995.[101] It is anticipated that even after 2005, if there had not been an AES competition and the new standard had not been widely accepted, problems associated with a multiplicity of strong encryption algorithms would have been more prevalent.

Although Camellia as a national algorithm would not have been accepted "as is" by the U.S. Government or U.S. standards bodies, it is plausible that Camellia or something like it would have become the foundation for a TDES replacement algorithm along a similar timeline.

[99] Tassey, 2017, op. cit., p. 228.

[100] Marco Giarratana, "The Birth of a New Industry: Entry by Start-ups and the Drivers of Firm Growth: the Case of Encryption Software," *Research Policy* Vol. 33, 2004, pp. 787–806;Marco Giarratana and Andrea Fosfuri, "Product Strategies and Survival in Schumpeterian Environments: Evidence from the U.S. Security Software Industry," *Organization Studies*, Volume 28, No. 06, pp. 909–929, 2007; Andrea Fosfuri and Marco Giarratana, "Resource Partitioning and Strategies in Markets For Technology," *Strategic Organization*, (forthcoming).

[101] The European Union's Data Protection Directive (officially Directive 95/46/EC) adopted in 1995; the Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub. L. 104–191, 110 Stat. 1936, enacted August 21, 1996); the Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*); the Sarbanes–Oxley Act of 2002 (Pub. L. 107–204, 116 Stat. 745, enacted July 30, 2002); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002; the Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5); and the Payment Card Industry Data Security Standard (PCI DSS), with multiple releases, 2004-2016.

In pre-survey interviews some industry representatives suggested that none of the NIST competition algorithms would have been developed without the AES competition. Instead, they posited that existing block ciphers such as Blowfish, RC5, and IDEA would have come into widespread use. The NIST competition uniquely forced industry and academia to produce innovative 128-bit block ciphers with 128-bit and greater keys, which previously was thought too difficult and computationally onerous to be practical. Although there would no doubt have been multiple alternatives to TDES, the evolution of a much stronger 128-bit cipher would have taken a more wandering path, and it is difficult to pinpoint when it may have appeared.

Market fragmentation generally heralds higher interoperability costs, as well as increased risk and complexity of supporting multiple non-standardized algorithms. Cryptography experts warn that, "complexity is the worst enemy of security." It was hypothesized that added complexity would increase risk for developers and users and, in turn, increase the probability of failed product roll-outs by developers and of breach losses by users.

In a possible version of the market fragmentation counterfactual, failed attempts to quickly fill the void in the absence of NIST's initiative might have materialized. If serious attacks had occurred during a period of market fragmentation, subject matter experts have offered historical examples of retrospectively imprudent attempts to advance insufficiently considered standards with serious cost consequences.[102]

One significant aspect of this period is that these alternatives represent what are called "national algorithms." NIST's competition was global and the winner was European. As such, AES has met with little adoption resistance in Europe and other parts of the globe. Lack of a global competition coupled with the proprietary development of "American" algorithms by U.S. entities, the widespread cross-border use of one U.S.-selected algorithm would likely never have emerged.

[102] Examples provided by subject matter experts include the first and second version of the *de facto* Secure Sockets Layer (SSL), intended to provide communications security over computer networks, and Wired Equivalent Privacy (WEP), a security algorithm introduced as part of the original IEEE 802.11 Wi-Fi standard ratified in 1997.

In summary, estimates of the size and temporal distribution of cost avoidance benefits from the AES program were the primary focus of the survey.  The nine-year fragmented market period is hypothetically characterized by competing domestic algorithms, slower diffusion of encryption technology, and limited international adoption.  Even beyond the nine-year period, the problems associated with the complexity of multiple strong encryption algorithms in the absence of AES would have been expected.  Government and commercial enterprises using encryption would not only have had to support more, possibly less efficient, domestic algorithms, they would likely be supporting separate algorithms for different sectors of the economy, and for each country (or block of countries such as the European Union).  Such fragmentation would have led to higher development, validation, testing, maintenance, and technical support costs, as well as increased the complexity and vulnerability of information systems.

Lack of U.S. leadership in this area would have impaired the competitive advantage of U.S. information technology companies, who were already struggling in the 1990s with restrictive export policies and the international perception that U.S. information technology products were subpar.  The U.S. information technology sector relies in part on government regulation and pronouncements to determine the direction of R&D efforts.  E-commerce, the internet, streaming services, and cloud computing all would have experienced significant interoperability issues that would have retarded U.S. technology advancements.  It is likely that, in this scenario, U.S. companies would not have dominated global technology business as they do today, or that internet-based goods and services would have been in such pervasive domestic use.

### 4.1.3 Segmenting the Survey Recipient Population

Two broad groups of likely beneficiaries of FIPS-197 include *consumers* of encryption systems and *developers* of encryption systems.

Encryption system consumers were further distinguished into two groups: *public sector* and *private sector* consumers of information encryption systems.  The range of encryption system hardware and software choices available to each group is different, and therefore the consequences of their choices have different economic effects.

Broadly, public sector consumers are limited by FIPS and other regulations, whereas private sector consumers are less restricted in their options.

For the purposes of the survey, public sector consumers include the CISOs of Federal agencies, the 50 states, and one territory. Private sector consumers include the CISOs, Chief Information Officers (CIOs), and/or data center managers of private sector firms that use encryption in their routine operations. These entities have historically been concentrated in the R&D intensive manufacturing sector, and in the financial, medical, and e-commerce service sectors. Professional cybersecurity associations whose members include private sector CISOs were invited to participate in the AES economic impacts survey.

As a result, the final survey instrument contained sets of survey questions for three distinct groups of potential respondents:

1. Government consumers—This group included Federal and state Chief Information Officers and any other government IT managers who were members of organizations distributing the survey. The survey for this group was 13 questions.
2. Private consumers—This group included companies that use a product containing encryption in their data centers or other services, but do not actually make or develop encryption products. Survey recipients included CISOs, CIOs, and other individuals with managerial or oversight responsibilities around encryption choices. The survey for this group was 26 questions.
3. Private integrators—This group included companies that develop and produce encryption hardware or software. It also included private academicians, independent encryption validation consultants, and independent cryptographers. The survey for this group was 20 questions.

## 4.2 Survey Execution

### 4.2.1 Survey Instrument Development

Based on communications with the cryptographic community, extensive background research, and the hypothesized benefits and counterfactual scenario, survey questions were formulated and iteratively improved with an eye to what could likely be collected from each of three different groups of beneficiaries: private sector consumers, public sector consumers, and developers and integrators of cryptographic hardware and software.

The full survey instrument is provided as Appendix B.

### 4.2.2 Survey Distribution

A professional online platform (research.net hosted by Survey Monkey) was selected to make distribution and survey completion simpler and more streamlined. This online approach greatly simplified the logistics of contacting and reminding the survey population to complete the survey. It also simplified data aggregation and analysis after the survey closed. Section 5 details the number of responses, their type and industry affiliations.

Direct survey contacts were contacted by email via the Survey Monkey platform. Selected members of participating organizations were contacted by email or through a form of communication deemed appropriate by them (e.g., periodic newsletters or announcements). Invitations to participate included a prefatory note from Donna Dodson, NIST's Chief Cybersecurity Advisor and Director of the National Cybersecurity Center of Excellence (NCCoE).

The open survey period ran from February 26, 2018 through April 9, 2018.

### 4.2.3 Direct and Indirect Access to Survey Recipients

A list of current Federal CIO's was obtained from NIST. The National Association of State Chief Information Officers (NASCIO) provided the point of contact for the CIOs or CISO's of 50 states and one territory.

NIST publishes validated certificate holders on its website. The list of AES CMVP holders was downloaded and analyzed to identify the entities holding the most active certificates and the most certificates overall, both active and historical. Emails and phone calls were made to the listed contacts to establish contact. Many of these contacts turned out to be technical managers who had a good understanding of how AES functioned, but had reduced visibility concerning business decisions such as the size of the IT budget and what portion of it was dedicated to encryption related activities and equipment. Nonetheless, these individuals provided good insights into the forces at play during the development and roll out of AES.

A number of organizations with interests in information security were contacted. The following organizations agreed to invite selected members of their organization to participate in the survey with the stipulation that the study authors would not have direct access to members' contact information:

- ANSI's Accredited Standards Committee X9 (ASC X9, Inc.)
- The Anti-Phishing Working Group (APWG)
- College of Healthcare Information Management Executives (CHIME)
- Cryptographic Module User Forum (CMUF)
- Common Criteria User Forum (CCUF)
- Executive Women's Forum on Information Security (EWF)
- Information Systems Audit and Control Association (ISACA)
- Information Systems Security Association (ISSA)
- IEEE's LAN/MAN Standards Committee (IEEE 802)
- National Council of Information Sharing and Analysis Centers (NCI ISAC)
- National Technology Security Coalition (NTSC).

Following an initial invitation, all organizations sent at least one reminder message to their members during the survey period.

# 5. Survey Results and Findings

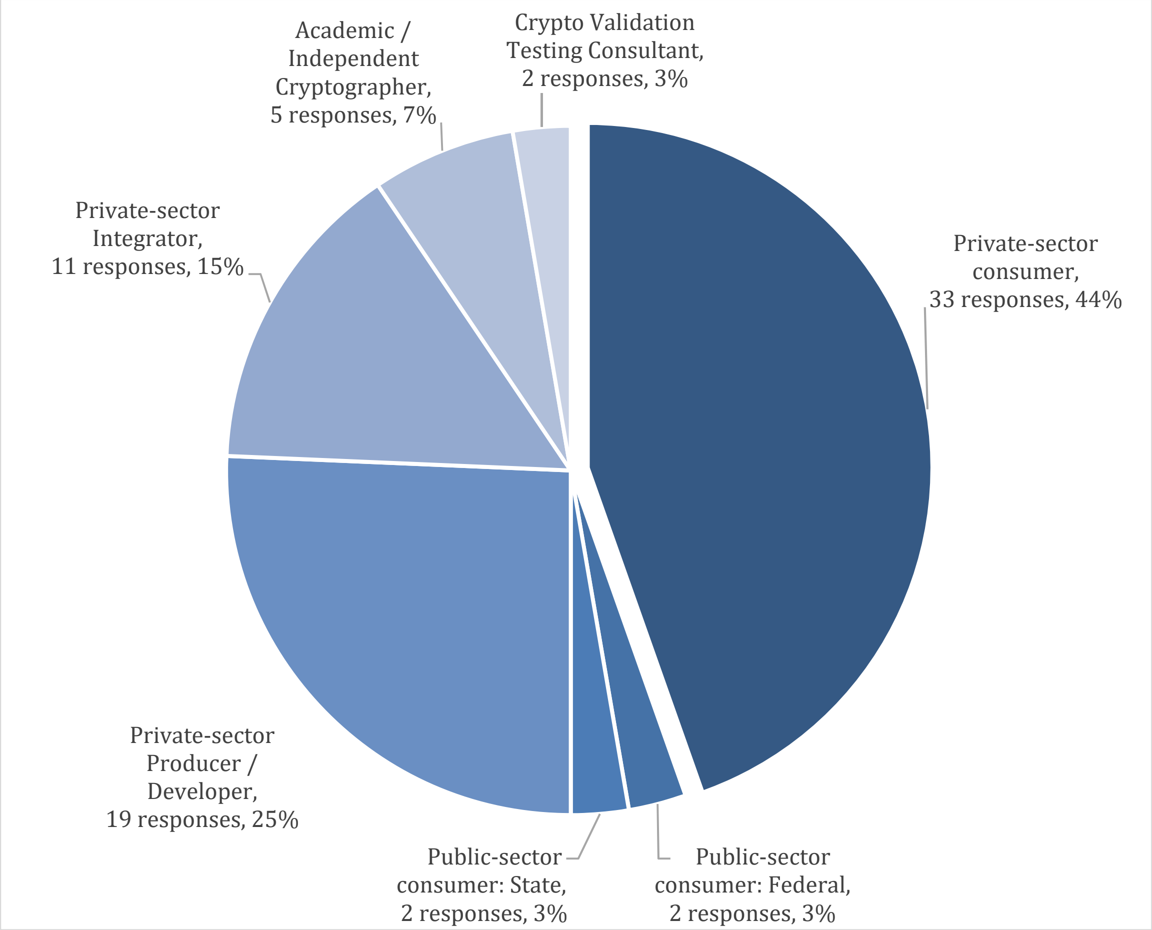
## 5.1 Survey Results

The survey contained three sets of questions for three distinct groups: 1) public sector consumers; 2) private sector consumers; and 3) cryptographic module producers, developers, and integrators. Survey responses were received from 169 respondents, of which 74 provided sufficient quantifiable information to allow for direct estimates of economic benefits. The 74 respondents consisted of the following:

- **Private sector consumers (demand side)—33 respondents**
  - Representing eight industry sectors: construction, manufacturing, retail trade, information technology, finance, scientific and technical services, health care, and arts and entertainment.
- **Public sector consumers (demand side)—4 respondents**
  - Federal Government—civilian and military agencies.
  - State, local, and tribal Governments.
- **Cryptographic module producers, developers, and integrators (supply side) —37 respondents**
  - Private-sector producers/developers of cryptographic modules.
  - Private-sector integrators—use externally made cryptographic modules to build other products.
  - Academic or Independent Cryptographers.
  - Cryptographic validation testing consultants (these individuals work closely with numerous private-sector producers, developers, and integrators).

Figure 5-1 shows in pie wedges the number of respondents of each type and its percentage of the 74 respondents, private sector consumers were the largest group of respondents, followed by private-sector producer/developers. The rate of response from Federal and state entities was considerably lower than anticipated.

*Figure 5-1. Survey Results: Seventy-Four (74) Respondents Reporting Quantifiable Benefits*



The additional 95 respondents can be characterized by type of respondent (private consumer, private producer/developer, private integrator, public consumer, academic or independent cryptographer, and cryptographic testing consultants) and their industrial classification category(ies). They answered various survey questions that could not be used to directly estimate their organizations' economic benefits. However, as explained fully in Section 5.3, information provided by all 169 respondents is used to extrapolate (from the economic benefits reported by the 74 respondents with directly quantifiable responses) the benefits of the 95 survey respondents who did not provide direct information about their benefits.

## 5.2 Introduction to Survey Findings

The survey findings are both qualitative and quantitative. The qualitative findings are matters of interest that can be used to verify or reject the pre-survey counterfactual hypotheses. The quantitative findings are used in calculations of the annual cost-avoidance benefits. Table 5-1 summarizes pre-survey hypotheses and indicates whether each finding has been assessed quantitatively, qualitatively, or both.

*Table 5-1. Anticipated Survey Findings*

| Pre-Survey Hypothesis | Qualitative | Quantitative |
|---|---|---|
| AES stimulated research & development. | X | X |
| Desire for key strength greater than TDES was prevalent. | X | |
| High switching costs postponed transition to AES. | X | |
| Absent AES, interoperability would have declined, and system complexity would have increased. | X | X |
| Absent AES, the risk of data breaches would have increased. | | X |
| CMVP certifications reduce procurement and sales-related costs. | | X |
| CMVP reduces the cost of module production and increased buyers' willingness to pay a premium. | | X |
| AES increased standard development process efficiency and improved time-to-market for dependent products. | | X |

## 5.2 Qualitative Discussion of Survey Findings

### 5.2.1 AES Stimulated Cryptographic Research and Development

The evidence that the AES program stimulated significant cryptographic research and development that would not have been undertaken as early, or on such a scale, is largely a matter of the economic logic of public goods (discussed in Section 3.1.3), the history of how the AES competition was implemented, and anecdotal evidence. Some private sector observers at the time recall paying close attention to the results of the AES competition as they unfolded and adjusting their product and service offerings accordingly, in some cases before the formal announcement of the competition winner.

The core process of requesting AES submissions, analyzing them, announcing and analyzing finalists, and selecting a winner ran from 1997 to 2000. Industry, government and academic sectors of the cryptographic community made analytical contributions, including concentrated attempts to break the submitted ciphers. The person-years of analytical support across the cryptographic community are thought to have been very large.[103] The benefits from the R&D stimulated by the AES program began accruing no earlier than 1998, after the competition was well under way, but before the formal announcement of a winner.

The relatively small quantity of benefits attributable to the early R&D stimulated by the AES program, and the timing of those benefits, are interpreted as evidence of cryptographic R&D stimulation. The benefits fall into three categories:

- Avoided costs of interoperability testing,
- Foregone "willingness to pay" benefits enjoyed by buyers of validated products,
- Costs avoided by producers due to implementation errors discovered in preparation for module validation.[104]

For the period 1998 to 2000 only, it is estimated that these benefits together account for approximately $5.8 million (2017 dollars) in R&D cost avoidance benefits.[105]

### 5.2.2 Desire for Key Strength > TDES Was Not a Common Sentiment

By the mid-1990s the cryptographic community—academia, government, and industry—knew that DES was vulnerable to attack, that TDES was therefore at increased risk, and that TDES had technical constraints in terms of its relatively small block size. Based on this, it was hypothesized that alternatives to TDES would be quickly adopted and that AES (or an equivalently strong and efficient block cipher) would have emerged as the block cipher of choice. Survey results did not confirm this supposition.

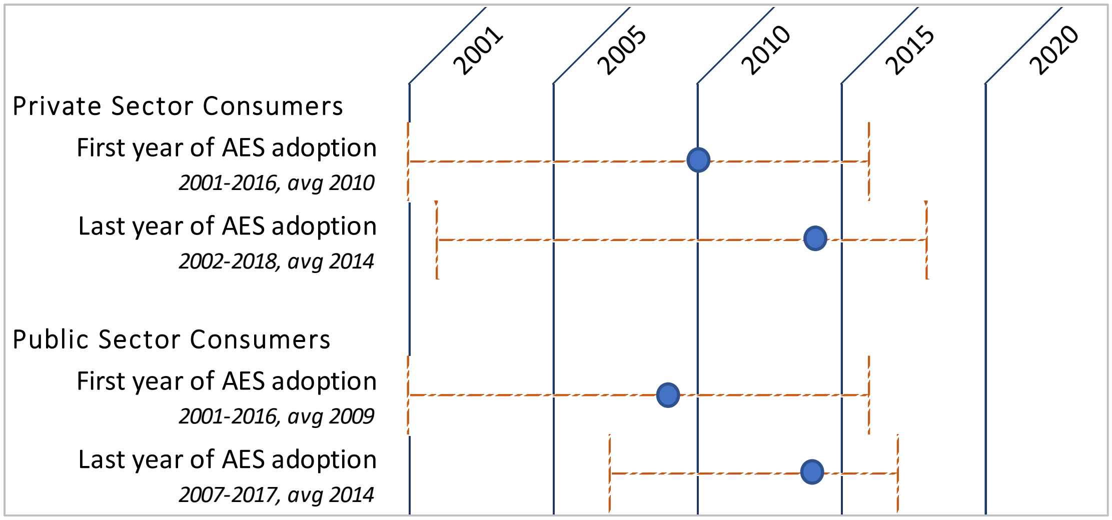
[103] One estimate put the contribution of NSA alone at 13 person-years of analysis.

[104] The survey instrument did not ask for R&D estimates. Companies offering FIPS-140 approved products from 1998-2000, or before, were assumed to be deeply engaged in following, or participating in, the AES competition and its results and thereby enjoyed R&D-related benefits captured in the three benefits categories available to respondents.

[105] The economic calculations and survey data supporting this amount are described in Section 5.3.

The survey questions for all recipients inquired about the first and last years in which their data centers adopted AES.[106] Respondents provided the ranges and averages shown in the graph below. As illustrated in Figure 5-2, although both private sector and public sector consumers have the same date range for first year adoption, on average public sector consumers adopted one year earlier than their private sector counterparts. For the last year of adoption, on average the private and public sectors' date of last AES adoption is the same.

*Figure 5-2. Survey Results: First and Last Years of AES Adoption: Range & Average*



Survey results indicate that AES tended to be first adopted by the private sector around eight years after it took effect as the Federal standard stronger than TDES. For private sector consumers of encryption systems, AES was finally being fully adopted by data centers only in the last few years, with an average year of adoption in 2014, more than a decade after AES was published as FIPS-197.[107] The pre-survey impression that an encryption algorithm stronger than TDES was popular seems to have been incorrect. Its perceived popularity did not result in a rush to transition.

[106] Seventy-nine private sector consumers of encryption systems provided the year in which their data centers first adopted AES. Seventy-six private sector consumers of encryption systems provided the year in which the last of its data centers adopted AES. Seven Federal agencies respondents provided first and last AES adoption dates.

[107] Seventy-six private sector consumers responded to this question. Responses ranged from 2003-2017 with a median of 2016 and a mode of 2017.

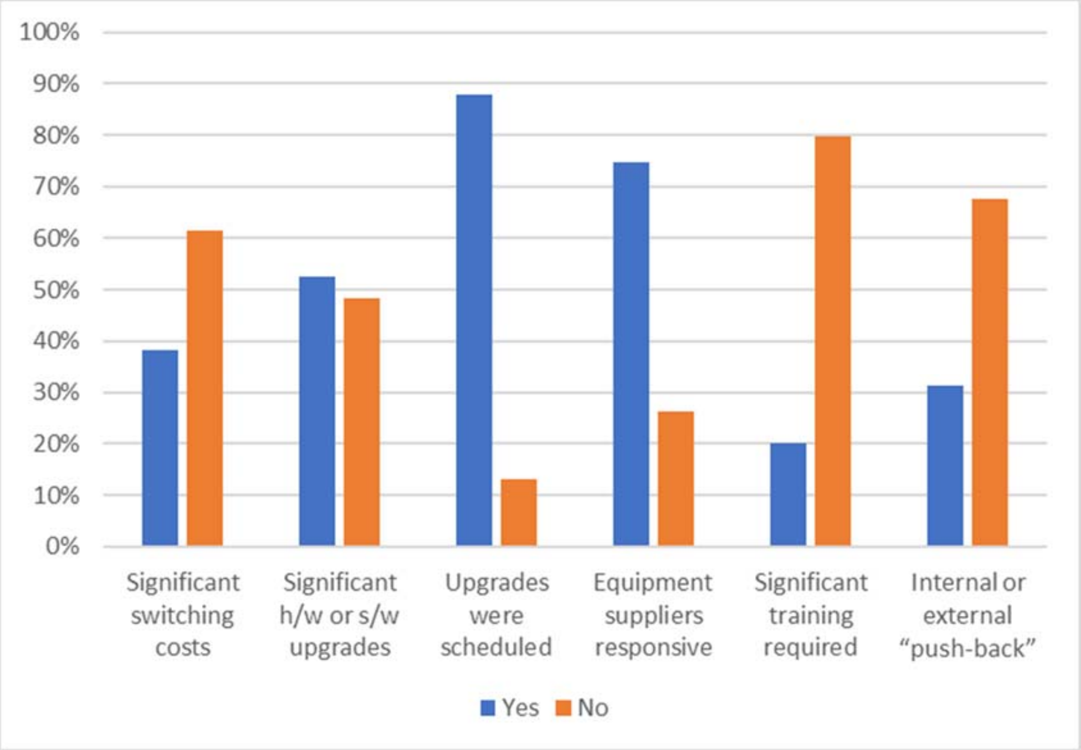
### 5.2.3 The Transition to AES was Postponed by High Switching Costs

The authors anticipated that some users would resist the shift from TDES to AES because of a variety of switching costs, especially, but not exclusively, associated with necessary security system hardware and software upgrades or replacements.[108] Economic theory concerning information system supply and demand (Section 3.1), as well as the case study of the transition from DES/TDES to AES encryption systems in the banking and finance sector (Appendix A), indicate that high switching costs among users and suppliers are likely to have played an important role in stifling the adoption AES-based encryption systems.

As indicated in Figure 5-3 below, survey results were mixed with regard to this issue, but the overall argument presented here affirms it. Public and private sector consumers were asked Yes/No questions regarding aspects of transitioning an encryption system from DES/TDES to AES. Private sector respondents were split on the existence of high switching costs as well as on whether they faced internal or external push-back in making the transition to AES.[109] More than three quarters believed that the transition required significant hardware or software upgrades, enough to merit scheduled work. As discussed in Section 5.2.2, respondents were slower to adopt AES than anticipated; 76% of 86 private sector encryption system consumer survey respondents affirmed that encryption system suppliers were responsive. It could be that over time the significance of switching costs declined when compared to other issues data center managers confronted.

[108] N. Ferguson, et. al., op. cit., p. 59: "If you have to be backward compatible or are locked into a 64-bit block size by other parts of the systems, [TDES] is still your best choice."
[109] Eighty-seven private sector respondents answered these questions.

*Figure 5-3. Survey Results: Transitioning from DES/TDES to AES*



Private sector consumer respondents were asked to identify the industry sector to which their organizations belonged according to the two-digit North American Industry Classification System (NAICS). Isolating answers about switching costs of those forty-one respondents identifying themselves with the banking and finance sector (NAICS 52), 41% affirmed high switching costs as a factor, while 59% rejected switching costs as a significant factor in AES-based encryption system adoption. Of those affirming high switching costs, their average number of years between first and last adoption of AES was 5.2 compared to a 4.4 year spread for those rejecting high switching costs. We can therefore deduce that for those who perceived higher switching costs for AES system adoption, full AES adoption took longer.

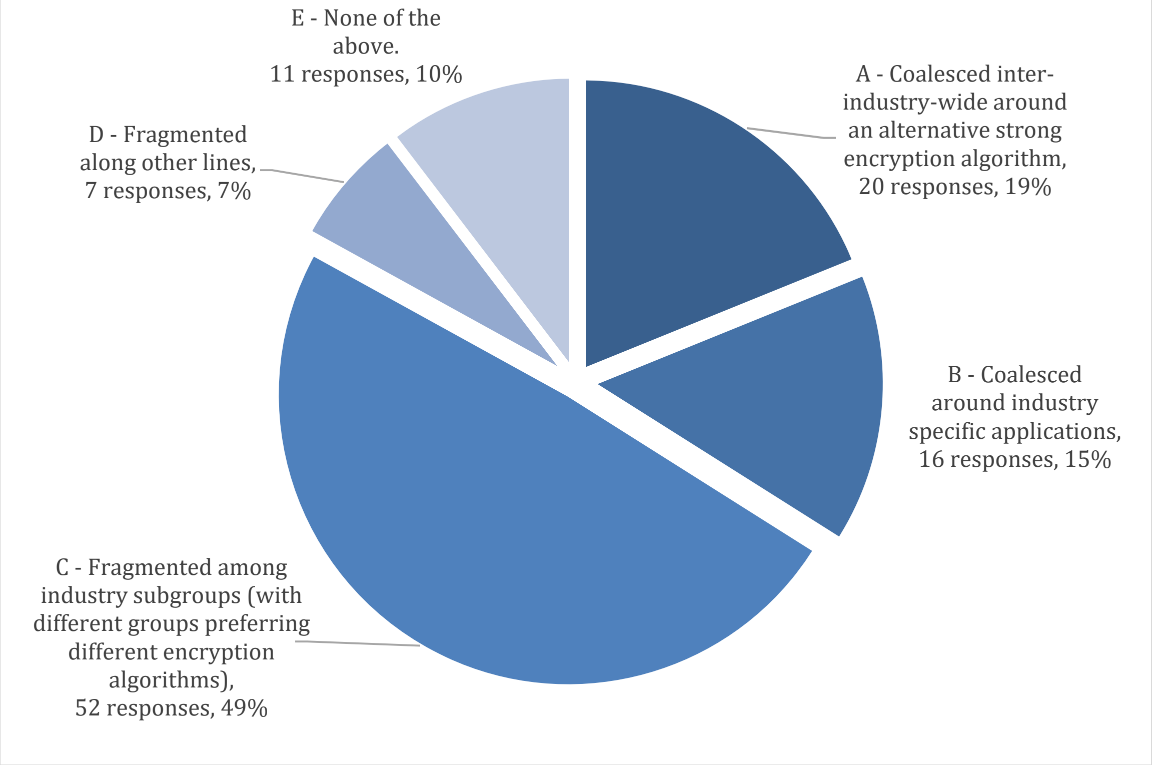
### 5.2.4 Absent AES, System Complexity and Risk Increase

Cryptography experts assert that, "complexity is the worst enemy of security."[110] It stands to reason that "absent AES," the increased complexity of ensuring interoperability, given an increase in the number of different strong encryption algorithms in use by

[110] Ferguson, et. al., op. cit., p.37.

different encryption systems, would increase risk for encryption system users. As indicated in Figure 5-4, by and large, these expectations were confirmed. Of the 59 encryption system users and producers who provided historical speculations about an absent AES market scenario, almost half (49%) indicated they believed option (C): the market would have fragmented among industry subgroups with different groups preferring different encryption algorithms. Options C, B, and D entail some significant degree of fragmentation, indicating that 71% of respondents (C, 49% + B, 15% + D, 7%) believed that market fragmentation (and therefore increased complexity of ensuring interoperability) was likely absent AES. Only 19% believed that an inter-industry-wide alternative strong encryption algorithm (Option A) would have emerged. In the counterfactual absence of AES, the most frequently suggested alternative by survey respondents was Twofish [111]

***Figure 5-4. Survey Results: Respondents' Most Likely "Absent AES" Scenario***



[111] While Twofish was a response to the AES competition, it is reasonable to assume that a version of it would have emerged as demand grew for algorithms with greater key strength than TDES.

Encryption system users were further asked how an increase in the number of different encryption networks affects the costs of maintaining interoperability. Of those responding to the question, 80% believed that costs rise linearly or exponentially as the number of different encryption networks increases. Additionally, respondents were asked if security risks increase as the number of different encryption networks increases. Again, 80% concurred that security risks would increase in this circumstance.

Finally, respondents were asked for the average number of data breaches (due to malware or hacking) reported to Federal or state authorities in the five-year period of 2013-2017. This response was used, in combination with the information regarding the relationship between breaches and the number of different encryption algorithms in use, to approximate the expected number of data breaches that respondents would have experienced absent AES. Out of all encryption system user respondents, 48% reported zero breaches for the period and 52% reported a positive number of breaches. The average number of breaches for all respondents was two breaches during the five-year period. For those reporting a positive average number of breaches, the average was four breaches over the five-year period.

## 5.3 Quantitative Findings

Section 5.3.1 describes the beneficiaries (survey respondents) and explains how benefits from NIST's program were estimated for 74 respondents to the survey and concludes with a time series of those benefits summed across all benefit categories annually, 1998-2017. Section 5.3.2 extrapolates the benefits for the sample of respondents to larger groups of beneficiaries in two stages, first to all 169 survey respondents, and then to the industries that all survey respondents represent. Section 5.4 describes NIST's costs for the AES program. The time series of costs and benefits described are used to calculate the overall economic impact metrics in Section 6.

### 5.3.1 Review of 74 Survey Respondents

As discussed in Section 5.1, of 169 survey responses, only 74 provided sufficient quantifiable information to allow for direct economic impact calculations. Thirty-three (33) respondents represented private sector consumers of encryption systems from eight industrial sectors; 4 public sector consumers of encryption systems representing Federal and state agencies; and 37 suppliers (producers, developers, integrators, and independent cryptographers and consultants) of cryptographic modules and encryption systems. Each of those 74 respondents typically did not provide enough information to quantify *all* of the types of benefits addressed with the survey; they often acknowledged that the benefits existed but did not attempt to provide the answers to the survey questions that would have allowed a quantitative estimate for each and every benefit category.

### 5.3.2 Directly Quantifiable Benefits and Methodology for 74 Respondents

The categories of measurable benefits gathered from the 74 respondents are summarized in Table 5-2. The table is followed by a discussion of the specific types of data gathered for each proposed benefit category and the methodology used for calculating those benefits.

*Table 5-2. Quantifiable Survey Topics Posed to Three Groups*

| Survey Questions Regarding | Demand side | | Supply side |
|---|---|---|---|
| | Private sector Consumers | Public Sector Consumers | Cryptographic Integrators |
| Benefits of faster AES processing speed | x | x | |
| Interoperability costs avoided | x | | |
| Interoperability testing costs avoided | | | x |
| Breach costs avoided | x | | |
| Avoided pre-acquisition costs for encryption hardware and software | x | | |
| Standards development costs avoided | x | x | x |
| Avoided lost profits from standards delay | | | x |
| Customers’ benefits from validation testing | | | x |
| Producers’ benefits from CA/MVP assisting implementation-error corrections | | | x |
| Benefits from the expansion of international markets | | | x |

<u>*Benefits of faster AES processing speed*</u>

Private and public sector consumers provided either known or estimated quantities for the following:

1. Their AES adoption date;

2. Their 2017 encryption budget;
3. Their 2017 encryption processing hours;
4. The annual growth rate in encryption processing hours since the adoption of AES; and
5. The multiple of the encryption budget needed to accommodate slower processing time in the counterfactual absence of AES.

Information provided by 24 consumers of cryptographic services allowed calculating the counterfactual avoided costs of encrypted data processing in 2017 constant dollars over the years since the respondent adopted AES.

*Interoperability costs avoided*

Private sector consumers of encryption systems provided estimates of the following:

1. Their AES adoption date;
2. Their 2017 encryption budget;
3. Their total 2017 encryption processing hours;
4. The annual growth rate in encryption processing hours since the adoption of AES; and
5. The increase in encryption processing hours needed to deal with interoperability issues across different encryption algorithms in the counterfactual absence of AES.

Based on the information provided, the avoided interoperability costs for the counterfactual scenario were calculated for 16 private sector consumers of encryption systems using the conservative assumption that entities would have only one additional algorithm and encryption network to deal with—a particularly conservative assumption because interoperability issues are typically described as increasing exponentially with the number of different algorithms.

*Interoperability testing costs avoided*

Producers, developers, and integrators of encryption products, were asked to quantify the following:

1. Their 2017 person-hours for interoperability testing across encryption modules and encryption containing products;
2. The full 2017 compensation (salary and benefits) for requisite personnel;

3. The multiple of the person hours required for interoperability testing absent AES; and
4. The estimated annual growth rates for the sales of encryption hardware and/or software since the first AES-containing product was sold.

Based on the information provided, a time series for the avoided costs of interoperability testing was estimated for 30 cryptographic suppliers.

*Breach costs avoided*

Private sector consumers provided either known or estimated quantities for the following:

1. The average number of breaches per year over the last five years; and
2. The relationship between number of breaches and number of interoperating encryption networks.

Most respondents that provided breach data also said that breaches would increase exponentially or linearly with the number of different encryption networks.[112, 113] Since none of the respondents were able to provide an estimate of the exponent for exponential relation, the avoided costs were calculated using the conservative assumption of a linear relationship and also the conservative assumption of just one more encryption network—i.e., one more different encryption algorithm—to deal with in the counterfactual absence of AES. The cost of a breach in the United States in nominal U.S. dollars for each of the years 2006 through 2016 was obtained from the Ponemon Institute.[114] The breach costs for 2003, 2004, 2005, and 2017 were extrapolated using ordinary least squares.[115] The

[112] Twenty-nine (29) of 36 private sector encryption system consumers responding concurred with the following statement: "As the number (n) of interoperating encryption networks increases, complexity increases, and as complexity increases (holding everything else constant) the risk of security breaches (with the number of breaches = s) increases." Twenty-four (24) of 27 concurring and responding to a question about the average number of breaches due to malware or hacking believe that the number of breaches (s) rises linearly or exponentially as the number (n) of interoperating encryption networks increases.

[113] Denoting the number of breaches with $y$ and the number of networks as $x$, an exponential relationship would mean $y = ax^b$ while a linear relationship would mean $y = a + \mathrm{b}x$, where $a$ and $b$ are constants.

[114] All breach cost estimates are based on the average total cost of a data breach for U.S. companies as reported in annual studies by The Ponemon Institute. Breach costs for 2006-2011 are reported in annual editions of *Annual Study: Cost of a Data Breach*. Breach costs for 2012-2016 are reported in annual editions of *Cost of Data Breach Study: Global Analysis* (2013-2017).

[115] Separate regression lines were fitted for the years 2006 through 2010 and the years 2011 through 2016. The fits of the regression lines were good. For the earlier period the $R^2 = 0.8233$, $F(1, 3) = 13.97$, probability of a greater $F = 0.0334$. For the later period, $R^2 = 0.9409$, $F(1, 4) = 63.68$, probability of a greater $F = 0.0013$.

nominal breach costs were converted to 2017 constant dollars using the chain-type price index for GDP.[116]

*Avoided pre-acquisition costs for encryption hardware and software*

Assuming that AES did not exist and some level of a proliferation of encryption algorithms occurred as a result, pre-acquisition costs (e.g., product search costs, qualification testing costs, and acceptance costs) for encryption hardware and software would probably have increased.  Private consumer respondents were asked to quantify or estimate the following:

1. The number of full time personnel in 2017 dedicated to encryption software and hardware pre-acquisition activities;
2. The multiple of those personnel that would have been required in 2017 in the counterfactual absence of AES; and
3. The full compensation (salary and benefits) in 2017 of a qualified full-time person performing these activities.

The information reported by 21 private sector consumers of encryption systems allowed calculating the avoided pre-acquisition costs in the counterfactual scenario absent AES.

*Avoided standards development costs*

All respondents were provided with a list of standards from the ISO, IETF, IEEE, and ANSI which contain normative references to AES.  All categories of respondents were asked to do the following:

1. Identify the standards they had worked on; and
2. Assuming the counterfactual absence of AES, estimate the number of
    a. additional hours that their personnel would have devoted to the standards work; and
    b. additional months that the particular standards would have been delayed.

The information provided by 17 suppliers and 19 consumers of encryption systems allowed the calculation of counterfactual standards development costs avoided and the

[116] The chain-type price index for gross domestic product (GDP) was obtained from Table B-3, "Quantity and price indexes for gross domestic product, and percent changes, 1967-2017", p. 536, *Economic Report of the President*, February 2018, Government Publishing Office, and on the Internet at www.gpo.gov/erp.

placement of the avoided costs in the appropriate years when the extra standards development work would have occurred.

*Avoided lost profits from standards delay*

Additional benefits exist for the supply-side respondents in the form of avoided lost profits from standards delay. Cryptographic suppliers were additionally asked to estimate the following:

1. The probable average delay in months, for the standards on which they had worked, in the counterfactual absence of AES; and
2. The probable average lost revenue per each month's delay.

The assumption is that a company's operations would have continued and the costs to produce products would have remained the same, but the sales would have been slowed. Sales would likely have slowed while products pending standards were withheld from the market or became outdated sitting on shelves. Hence, the lost revenues during a month's delay translate to a loss in profits for that month. Given the actual release dates for the standards and the number of months they would have been delayed in the counterfactual scenario, the benefit of the estimated avoided lost profits could be added to the time series of AES benefits for ten cryptographic suppliers.

*Customers' benefits from validation testing*

Supply-side respondents (cryptographic producers, developers, and integrators) provided information about their customers' benefits from validation testing as reflected in the prices paid by the buyers of encryption hardware and software. FIPS-140-2 validation testing is valuable to module producers because it provides valuable assurances to buyers that producers' encryption hardware and software conform to high standards of cryptographic security. These assurances mean that buyers are willing to pay more for the validated product. Respondents estimated the following:

1. The value of these validation-testing assurances, as a percent of module average price ranges that they provided for 2017;
2. The years in which their sales of AES-related FIPS validated hardware and/or software began; and
3. The growth rates for sales of the FIPS validated encryption hardware and/or software.

From the information provided by 26 supply-side respondents, a time series was constructed of the lost value that was avoided by buyers of the hardware or software modules, given that validation testing increases buyers' willingness to pay.

*Producers' benefits from CA/MVP assisting implementation-error corrections*

FIPS-140-2 validation testing is valuable to cryptographic hardware and software module producers because it uncovers or confirms implementation errors that module producers would otherwise need to correct, for example, by sending technicians to test and fix bugs that were not fixed prior to module deployment. At a minimum, the value of FIPS validation testing is the cost to producers of correcting errors found (or confirmed) in the validation process. That is because the validation testing in any year is an investment in the new product or products being tested. The present discounted value, to the developer and producer, of the future returns on that investment during the year must be at least equal to the testing cost (so that benefits at least equal the costs). Thus, a lower bound on the value in a representative year is provided by a respondent's costs of correcting implementation errors found or confirmed in the validation process. Cryptographic producers provided estimates, across all modules validated by their organization in a representative year, of the following:

1. The total number of person-hours dedicated to correcting implementation errors found or confirmed in the validation process; and
2. The average annual full-time compensation (salary plus benefits) of personnel with the appropriate capability to perform the necessary tasks.

With the information provided by 27 producers, a time series of the avoided lost value was constructed to provide estimates of average annual benefits over the years since sales of the AES-related FIPS-validated products began. Some suppliers reported selling FIPS-validated products beginning in the period before the availability of knowledge about the strong encryption standards emerged during the AES competition; for those respondents the benefits of implementation-error correction were not begun until the AES era was underway starting in 2001.

*Benefits from expansion of international markets*

The development and promulgation of AES increased worldwide demand for products and services incorporating strong symmetric block encryption. Cryptographic suppliers provided estimates of the following:

1. Information about the 2017 sales of encryption-containing modules;
2. The years in which their sales of AES-related FIPS validated hardware and/or software began;
3. The average annual growth rate for their strong cryptographic hardware and software module sales;
4. The average annual sales growth rate that would have occurred in the absence of AES; and
5. The AES-related standards that supported the respondent's sales.

The foregoing information, provided by 15 suppliers, allowed estimation of the difference between the actual time series for sales and what the time series would have been in the absence of AES. Beginning at the release time for the AES-related standards supporting the sales, and holding the producer's costs constant,[117] the time series of the difference between actual sales growth and counterfactual retarded sales growth provided a time series of benefits. These benefits were avoided lost profits—lost profits that would have resulted as sales growth in the counterfactual scenario slowed due to the loss of the AES effect on international standards and the expansion of international markets for cryptographic products and services.

For each of the 74 survey respondents reporting benefits from any of the areas described above in a given year, benefits were summed and accumulated across all respondents. Table 5-3 shows the time series of AES benefits for all respondents in a given year, in 2017 constant dollars, 1998 to 2017.

[117] This is a sensible first-order estimation given the way the production of encryption products and services works with the on-boarding of new clients to use the products developed. The time series of costs for the supplier stays the same, but the time series for a portion of the sales is shifted into the future periods.

*Table 5-3. AES Benefits for 74 Survey Respondents*

| Year | Total Benefit*<br>(Constant 2017 dollars) |
|---|---|
| 1998 | 1,841,514 |
| 1999 | 1,934,932 |
| 2000 | 2,046,763 |
| 2001 | 7,688,332 |
| 2002 | 15,920,284 |
| 2003 | 34,271,978 |
| 2004 | 46,318,887 |
| 2005 | 67,439,960 |
| 2006 | 50,839,308 |
| 2007 | 82,014,903 |
| 2008 | 80,076,964 |
| 2009 | 91,392,576 |
| 2010 | 175,000,000 |
| 2011 | 189,500,000 |
| 2012 | 184,100,000 |
| 2013 | 199,900,000 |
| 2014 | 296,400,000 |
| 2015 | 321,700,000 |
| 2016 | 370,400,000 |
| 2017 | 399,400,000 |

*For 74 respondents who provided sufficiently quantifiable responses.

The benefits calculated for the 74 respondents in Table 5-3 are conservative totals for many reasons. Prominent among them are the underestimates for the supply-side respondents of buyers' benefits from validation testing and benefits from expansion of international markets. Note that the benefits before 2002 reflect the benefits of the AES competition, that is, the benefits for the R&D cost avoidance by cryptographic suppliers—producers, developers, integrators, academics, and consultants. The years with pronounced jumps in benefits reflect years with a large number of new beneficiaries in the counterfactual scenario because of their AES adoption dates (for consumer organizations in the sample) or because of the beginning of FIPS-validated sales (for producer organizations in the sample).

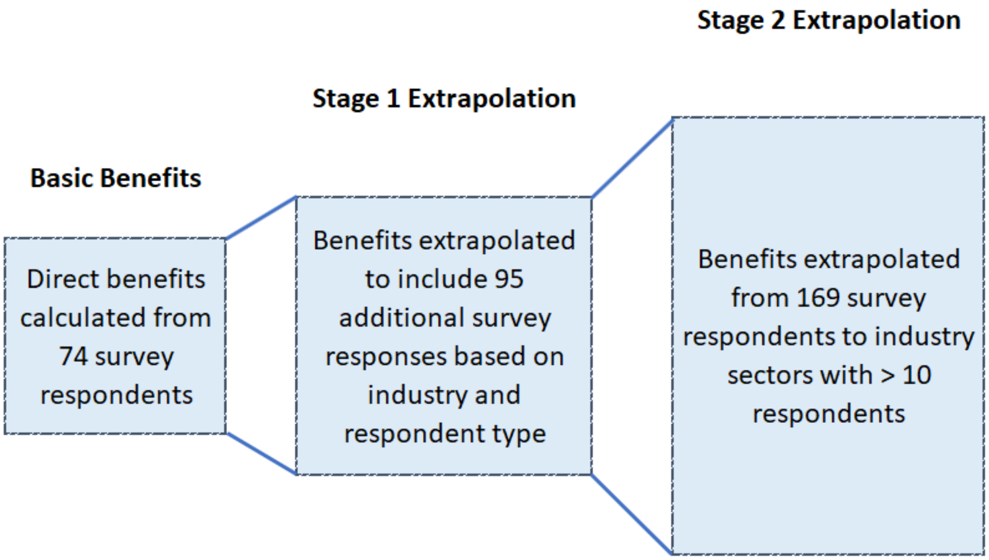
In the following Section 5.3.3, these benefits are extrapolated to larger samples (described in Section 5.1), and when the extrapolation is complete, we extrapolate from the cumulated present values of benefits in 2017 for the 74 observations to the analogous cumulative benefits for the larger samples. Thus, our extrapolations will not provide the individual, yearly amounts of each category of benefits over the period from 1996 through 2017, but their total, cumulated at the social rate of return to have their present value in 2017 dollars.

### 5.3.3 Extrapolation of Benefits to Larger Samples

As illustrated in Figure 5-5, the extrapolation of benefits from the 74 respondents discussed in Section 5.3.2 to larger samples takes place in the following two stages:

- First, the benefits based on the 74 respondents reported in the section above are extrapolated to an additional 95 survey respondents. Those 95 respondents did not provide information from which cost avoidance benefits could be directly estimated, but they did provide enough information to allow estimation of their benefits by using an estimated model of the benefits for the 74 respondents with direct information about benefits;
- Second, the benefits are extrapolated for the industrial sectors to which the 169 survey respondents belong.

***Figure 5-5: Extrapolation of Benefits in Two Stages***


Stage 2 Extrapolation
Stage 1 Extrapolation
Basic Benefits
Direct benefits calculated from 74 survey respondents
Benefits extrapolated to include 95 additional survey responses based on industry and respondent type
Benefits extrapolated from 169 survey respondents to industry sectors with > 10 respondents

Briefly, a first stage extrapolation begins with the estimates from the 74 survey respondents, discussed in the preceding Section 5.3.2, and assumes that an additional 95 survey respondents who identified themselves by industry sector  (2-digit NAICS code), and type of respondent (private consumer, private producer/developer, private integrator, public consumer, academic or independent cryptographer, and cryptographic testing consultants), would have provided statistically similar responses to those provided by respondents of the same type and in the same industry sector (A full explanation of this approach is explained in Appendix E.)  For each of the 74 respondents, the present value of all the benefits (in 2017 constant dollars) they reported between 1998 and 2017 was calculated as of 2017 (hereafter referred to as an organization's "cumulative benefits"). Then, the question is statistically posed: "Do the cumulative benefits of each of the 74 survey respondents vary significantly on the basis of their industry sector and/or type of respondent?" The answer is "yes;" statistically speaking, the cumulative benefits can be explained with a model that has industry sector and type of respondent as the explanatory variables.  That estimated model is used to predict the cumulative benefits of the additional 95 survey respondents.

Accordingly, summing the benefits for the 169 individuals that responded to the survey—74 with information of at least some of their quantitative benefits and another 95 with sufficient categorizing information (respondent type and industry) used in our estimated model of benefits—the cumulative benefits for all 169 survey respondents is $8,899,000,000.[118]

A second-stage extrapolation used the cumulative benefits of the 169 survey respondents discussed above, and information about the industrial sector to which the respondents belong, to estimate the benefits of the AES program for large sectors of the U.S. economy represented by survey respondents.  Briefly, the employment size of each respondent's organization (in some cases reported and in other cases estimated) was used to estimate the proportion of the sector's employment taken by the respondents belonging to that industrial sector.  (This procedure was only used where the number (*n*) of the 169 respondents belonging to an industrial sector was ten or greater.)  Benefits were extrapolated for the following sectors: NAICS 31-33—Manufacturing (*n* = 45), NAICS 51—Information (*n* = 47), NAICS 52—Finance and insurance (*n* = 42), NAICS 54—

[118] The economic impact metrics for this benefit stream are presented in Section 6, Table 6-3.

Professional, scientific, and technical services (*n* = 41), NAICS 61—Educational services (*n* = 12), NAICS 62—Health care and social assistance (*n* = 13), and NAICS 92—Public administration (*n* = 16).

Each industry sector is assigned all the cumulative benefits for the *n* survey respondents in that sector (*n* of 169) as described in the first-stage extrapolation above. For example, looking at the Manufacturing row of Table 5-4, the cumulative benefits (1998-2017) for the 45 respondents reporting in that industry sector are estimated to be $907,000,000 (column 4). The total employment reported or estimated for those 45 survey respondents is approximately 1.8 million (column 3) and the total employment for the manufacturing sector in 2017 is reported as approximately 12.3 million (column 5). Using the proportion of total industry sector employment represented by the 45 survey respondents belonging to that sector (column 6), we estimate cumulative benefits for the manufacturing sector as a whole (column 7) by dividing the proportion of total industry sector employment represented by the 45 survey respondents (column 6) into the value of the cumulative benefits estimated for the 45 survey respondents. Thus, (the *n* respondents' benefits in the sector) / (proportion of the sector's employment taken by the *n* respondents) = (benefits for the sector).

***Table 5-4. Extrapolation of AES Benefits to the Economy***[119]

| (1)<br>Sector (Industry classification, NAICS) | (2)<br>*n* | (3)<br>Total 2017 employment for the *n* respondents | (4)<br>Total $PVbnft2017_{sector}$ for the *n* respondents (2017 dollars) | (5)<br>Total 2017 Employment for the sector* | (6)<br>Proportion of sector employment for the *n* respondents | (7)<br>Estimated *PVbnft2017* for the sector (2017 dollars) |
|---|---|---|---|---|---|---|
| Manufacturing (31-33) | 45 | 1,773,633 | 907,000,000 | 12,299,600 | 0.1442 | 6,290,000,000 |
| Information (51) | 47 | 1,624,431 | 1,090,000,000 | 2,800,500 | 0.5801 | 1,879,000,000 |
| Finance and Insurance (52) | 42 | 544,272 | 2,690,000,000 | 5,857,390 | 0.09292 | 28,950,000,000 |
| Professional, Scientific, and Technical Services (54) | 41 | 394,052 | 2,030,000,000 | 8,850,270 | 0.04452 | 45,600,000,000 |

[119] The economic impact metrics for this estimate's benefit stream are presented in Section 6, Table 6-3.

| | | | | | | |
|---|---|---|---|---|---|---|
| Educational Services (61) | 12 | 48,756 | 87,600,000 | 13,042,580 | 0.003738 | 23,430,000,000 |
| Health Care and Social Assistance (62) | 13 | 90,154 | 555,000,000 | 20,208,050 | 0.004461 | 124,400,000,000 |
| Public Administration (NAICS 92, OES 99) | 16 | 181,127 | 376,000,000 | 9,661,980 | 0.01875 | 20,050,000,000 |

* United States Department of Labor, Bureau of Labor Statistics, Occupational Employment Statistics, "May 2017 National Industry-Specific Occupational Employment and Wage Estimates," https://www.bls.gov/oes/current/oessrci.htm, accessed May 4, 2018.

Summing the benefits for the all sectors shown in Table 5-4, column 7, gives the total extrapolated AES benefits for the sectors with ten or more respondents. Those total benefits equal $250,600,000,000. These estimated benefits are calculated *as if* annual benefits had been invested at the OMB-specified rate of 7% and cumulated over two decades. Since benefits were not estimated for the sectors of the economy where the survey had fewer than ten respondents, the sum of the estimated benefits for the sectors shown in the table is a lower bound of the total benefits for the economy.

## 5.4 NIST's Costs for the AES program

NIST provided the total AES program annual costs from the incipiency of the program in 1996 through 2017. Those costs, for total compensation of labor and the overhead costs, included costs for the research, the standardization activities, and the updating of modes of operation and the development of new modes of operation to accommodate the increased block size of the AES algorithm. Also included were the costs of AES-related validation work. The annual costs were provided in 2012 constant dollars, and the costs were converted to 2017 constant dollars.[120] Table 5-5 shows the time series of NIST's annual costs for the AES program.

[120] The annual costs were converted to 2017 constant dollars using the using the chain-type price index for gross domestic product (GDP), Table B-3, "Quantity and price indexes for gross domestic product, and percent changes, 1967-2017", p. 536, *Economic Report of the President*, February 2018. Government Printing Office, and on the Internet at www.gpo.gov/erp.

*Table 5-5. Time Series of NIST's AES program Costs*

| | Year | NIST's Total Annual AES Program Costs (Constant 2017 Dollars) |
|---|---|---|
| AES competition & development | 1996 | $ 349,272 |
| | 1997 | 2,655,110 |
| | 1998 | 2,655,110 |
| | 1999 | 2,655,110 |
| | 2000 | 2,655,110 |
| | 2001 | 2,655,110 |
| | 2002 | 4,216,052 |
| | 2003 | 3,016,240 |
| | 2004 | 3,182,252 |
| | 2005 | 3,335,327 |
| | 2006 | 2,563,480 |
| | 2007 | 2,836,214 |
| | 2008 | 2,497,722 |
| | 2009 | 2,352,193 |
| | 2010 | 2,401,781 |
| | 2011 | 2,436,276 |
| | 2012 | 2,482,630 |
| | 2013 | 2,521,438 |
| | 2014 | 2,626,004 |
| | 2015 | 2,626,004 |
| | 2016 | 2,677,748 |
| | 2017 | 2,730,570 |

# 6. Economic Impact of the AES program, 1996-2017

## 6.1 Economic Impact Metrics

The present value, at the onset of the AES program in 1996, of the time series of NIST's annual costs for the AES program is $30,633,590 in 2017 constant dollars.[121] The time series of AES benefits for only the 74 survey respondents at the onset of the AES program in 1966 (from Table 5-3 above) is $875,133,112 in 2017 constant dollars.[122]

*Table 6-1. Evaluation Metrics for the 74 Respondents*

| | |
|---|---|
| Benefit-to-cost ratio | 28.6 |
| Net present value | $844,500,000 |
| Internal rate of return | 0.807 or 80.7% |

Table 6-1 summarizes conventional evaluation metrics using only the benefits for the 74 respondents. Based solely on the benefits reported for the 74 respondents, the present value of the benefits divided by the present value of the costs, the benefit-to-cost ratio, is 28.57; the surplus of benefits over the costs, the net present value, for NIST's AES program is $844,499,522. The internal rate of return for the AES program—the rate at which NIST's investments in the AES program is growing—is 0.807 or 80.7%.[123]

*Table 6-2. Extrapolated Evaluation Metrics for the 169 Survey Respondents*

| | |
|---|---|
| Benefit-to-cost ratio | 70.2 |
| Net present value | $8,772,000,000 |

[121] The present value of NIST's costs is the amount that would have to be invested, at the beginning of the investment project and earning the social required rate of return of 7% per year (as used in the previous NIST evaluation studies—see Albert N. Link and John T. Scott, *The Theory and Practice of Public-Sector R&D Economic Impact Analysis*, NIST Planning Report #11-1, January 2012, National Institute of Standards and Technology, U.S. Department of Commerce; the 7% social discount rate was introduced in Office of Management and Budget (OMB), Circular no A-94: Guidelines and discount rates for benefit-cost analysis of Federal programs, Washington D.C.: Government Printing Office, 1992), in order to release in each year an amount equal to the cost in that year. Thus, the present value of the costs is $\sum_{t=0}^{T} COST_t / (1.07)^t$ where T = 2017 – 1996 = 21.

[122] The present value of the benefits for our 74 respondents is that amount that if invested at 7% per annum at the beginning of the investment project would release in each year an amount equal to the benefits in that year. Thus, the present value of the benefits is $\sum_{t=0}^{T} benefit_t / (1.07)^t$ where T = 2017 – 1996 = 21.

[123] The internal rate of return is the interest rate that discounts the stream of benefits to the present value of the stream of costs. Thus, it is $r$ such that $\sum_{t=0}^{T} COST_t / (1+r)^t = \sum_{t=0}^{T} benefit_t / (1+r)^t$.

| | |
|---|---|
| Alternative internal rate of return* | 0.310 or 31.0% |

* For comparative purposes, the alternative internal rate of return for the 74 survey respondents presented in Table 6-1, is 25.5%.

Table 6-2 summarizes conventional evaluation metrics using the extrapolated benefits for 169 respondents (the Stage 1 extrapolation described in Section 5.3.3). The present value in 2017 of NIST's costs over the years from 1996 through 2017, Present Value NIST Costs$_{2017}$, is $126,800,000.[124] Using the estimated AES benefits for the sample of 169 organizations, the benefit-to-cost ratio, Benefit$_{2017}$/Cost$_{2017}$, is $8,899,000,000 / $126,800,000 = 70.18. The net present value, Net Present Value$_{2017}$, is $8,772,000,000. For reasons explained in Appendix D (Understanding the Alternative IRR), an "alternative internal rate of return" of 0.310 or 31.0% is computed rather than the conventional internal rate of return. [125]

***Table 6-3. Evaluation Metrics for the Extrapolation of 169 Survey Responses to Selected Sectors of the U.S. Economy***[126]

| | |
|---|---|
| Benefit-to-cost ratio | 1976.3 |
| (Net present value)$_{2017}$ | $250,473,200,000 |
| Alternative internal rate of return* | 53.6% |

* For comparative purposes, the alternative internal rate of return for the 74 survey respondents presented in Table 6-1, is 25.5%.

Table 6-3 summarizes the metrics for the extrapolation to the economy-wide effect of NIST's investments. Summing the benefits for the all sectors shown in column 7 of Table 5-4 (Section 5.3.3) gives the total extrapolated AES benefits for the sectors with ten or more respondents. Those total benefits equal $250,600,000,000. Recall that these are benefits invested and cumulated over two decades. In the sense that benefits for the sectors of the economy where we have fewer than ten respondents are not estimated, the

[124] Thus, the present value in 2017 of NIST's AES costs provided in Table 1 is $\sum_{t=1996}^{2017} COST_t \times (1.07)^{2017-t}$

[125] This alternative internal rate of return is the solution $r$ to the equation: $(30{,}633{,}590)*(1+r)^{21} = 8{,}899{,}000{,}000$.

[126] Notes: (Present value in 2017 of AES economy-wide benefits cumulated from 1998)$_{\text{lower bound}}$ = $250,600,000,000. (Present value in 2017 of NIST's AES costs cumulated from 1996) = $126,800,000. (AES Economy-wide Benefit-to-Cost Ratio)$_{\text{2017, lower bound}}$ = 1976.3. (AES Economy-wide Net Present Value)$_{\text{2017, lower bound}}$ = $250,473,200,000. Alternative internal rate of return = 0.536 or 53.6%; it is the solution $r$ to the equation: $(30{,}633{,}590)*(1+r)^{21} = 250{,}600{,}000{,}000$.

sum of the estimated benefits for the sectors shown in the table are a lower bound of the total benefits for the economy. The cumulated present value amount as of 2017 of NIST's costs was defined and discussed in the earlier discussion. We then have a lower-bound estimate of the AES benefit-to-cost ratio for the economy: the sum of the sector benefits in Table 5-4, column 7 (from Section 5.3.3) divided by the present value in 2017 of NIST's costs for the AES program over the years from 1996 through 2017; the ratio is \$250,600,000,000 / \$126,800,000 = 1976.34. A lower bound AES economy-wide alternative internal rate of return for NIST's investments is 0.536 or 53.6%.

## 6.2 Discussion and Conclusion

The benefits of roughly \$250 billion are substantial, but they are not unusually large. First, observe that those benefits are a cumulative total of annual benefits earning interest at the social rate of return over two decades. To provide perspective, consider that for fiscal year 2017, Microsoft had \$90.0 billion in revenue and \$22.3 billion in operating income.[127] A company that annually earned operating income of \$20 billion in 2017 constant dollars over the two decades from 1998 through 2017 would have \$820 billion by 2017 if the annual income were invested and cumulated at 7%.[128]

Second, in many ways the estimated benefit is a very conservative, lower-bound estimate. This is the result both of self-imposed restrictions and limits on required data. Some of the most important limitations were the following:

1. *Self-imposed limit on wider economic extrapolations*—The \$250 billion as of 2017 was projected for just those sectors of the economy where there were 10 or more respondents to the survey about the AES benefits.

2. *Partial responses from survey participants*—Many of the respondents, while providing enough information to quantify some of their benefits, also acknowledged other benefits but could not, or in any case did not, provide the information necessary to quantify those benefits. For example, many respondents reported that buyers were willing to pay more for FIPS validated (CA/MVP)

[127] https://www.microsoft.com/investor/reports/ar17/index.html. Accessed May 5, 2018

[128] Note the analogy with our earlier computation where the present value of an organization's benefits in 2017 is $PVbnft_{2017} = \sum_{t=1998}^{2017} benefit_t \times (1.07)^{2017-t}$.

cryptographic hardware or software, yet for various reasons could not provide all of the information needed to convert into quantified benefits their reported estimate of the percentage of the value of their cryptographic products and services that was due to the FIPS validation.

Reasons included the confidentiality of the information in many cases, but also for many products, the cryptographic capabilities are built in and are not priced separately. As a result, respondents would not attempt to provide the information about the annual revenues earned from the cryptographic hardware and/or software modules that they produced.

Further, many of the supply-side respondents (30) provided very complete information about the pricing of their cryptographic modules, but then did not provide detailed information about the number of clients that were paying for the use of those modules. As a consequence, the measured benefits greatly underestimate the supply-side respondents' AES benefits resulting, because their customers value validation testing. The benefits for supply-side respondents because AES stimulated the expansion of their international markets are also greatly underestimated, because of the same incompleteness in the information about the annual revenues that are generated by the respondents' cryptographic hardware and software modules.

3. *Authors use of lower-bound or conservative interpretations of survey data*—One major example lies with the data regarding consumers of cryptographic services, and their AES benefits from reduced interoperability costs and from reduced numbers of breaches. Respondents typically held the view that interoperability costs and security breaches increase when their data centers must deal with a greater number of different encryption networks that use different encryption algorithms. Many of the respondents reported that such complexity causes both interoperability costs and breaches to increase exponentially. Some reported that the costs and the breaches would increase linearly with the number of different encryption networks with which their data centers deal. No respondent, however, could quantify the exponent for the commonly expected exponential increases, so

> to be very conservative, linear relationships were assumed when estimating the avoided interoperability costs and the avoided breaches.
>
> Further, although many respondents reported that absent AES there would have been many additional strong encryption algorithms in use, the authors conservatively assumed that absent AES there would have been just one additional strong encryption algorithm with which the data centers had to deal.

Evidence supports that estimated AES benefits are clearly underestimates. The survey responses support the conclusion that NIST's investment in AES has been repaid many times over, with economy-wide benefits exceeding NIST's costs by a multiple well in excess of the extrapolated benefit-to-cost ratio of roughly 2,000.[129]

[129] Although the conservative lower bound refers directly to the comparison of the benefits to NIST's costs, the overall picture of a large social benefit relative to costs would be essentially unchanged if other social costs, such as the National Security Agency's contribution to the development of AES, were included.

# 7. Overall Economic Impact Assessment Conclusions

In 1996, members of economic policy establishment are reported to have been in the midst a long-brewing policy crisis that pitted Federal law enforcement and intelligence agencies against commercial encryption hardware and software developers that were unhappy with export controls.[130] That year NIST launched an innovative effort to replace the Federal Government's standard encryption algorithm—DES, FIPS-46-3—by means of an open international competition. The competition was the first of its kind, through which NIST would ultimately choose an algorithm designed by two Belgian cryptographers. This significantly stronger algorithm would be endorsed by NIST as the Advanced Encryption Standard, FIPS-197, in 2001. The rudiments of cryptography, and the many facets of its role in industry—from both the developers' and users' perspectives—are discussed as background in the preliminary chapters of this report.

This study aims to evaluate NIST's AES program initiative as though it were a private sector investment decision and provide economic valuations for Net Present Value (NPV), Internal Rate of Return (IRR) and Benefit-to-Cost ratio (B/C). By treating the Federal investment in the AES program as though it were a private investment decision, analysis of the survey data collected for the study supports the conclusion that NIST's investment of public resources has been successful.

The NPV metric (for our lower-bound economic impact approach (Section 6.1, Table 6-1), based only on the estimates provided by 74 survey respondents), says in effect that if, in 1996, NIST AES program managers could have projected the actual timing and size of the economic benefits (costs avoided) they would have valued the project at $844,500,000, net of costs incurred. To provide perspective about the performance of the AES program, consider 12 other NIST infra-technology projects for which NPV was calculated (1999-2011). For the 12 projects, the median NPV was $48.5M, with NPV's ranging from $3.5M to $773M.[131]

[130] Levy, op. cit., and Smid, op. cit.

[131] https://www.nist.gov/director/outputs-and-outcomes-nist-laboratory-research, updated by the authors.

Similarly, another investment decision metric, the IRR, indicates that the return on NIST's AES investment over the period from 1996 to 2017 has been approximately 81%. The IRR is the interest rate (also called the "discount rate") that would reduce the projected NPV of the AES program in 1996 to zero and reduce the B/C ratio to one. Stated differently, it is the discount rate for which the investment would breakeven. In contrast, the hurdle rate for public investment projects is 7%. That hurdle rate is the actual discount rate, also called the social required rate of return, that is used to value public investments and becomes a threshold rate of return for a public investment project. As a guide to making an investment decision on a public or private project, if the IRR is higher than the discount rate, the project is acceptable because the project earns a rate of return greater than its cost of capital. An IRR of 81% is obviously well over the government-mandated threshold of a 7% rate of return. For comparison with the 81% IRR for the AES program, consider 37 NIST infra-technology projects evaluated for IRR over as many years; for those projects, the median IRR was 117%, and the rates ranged from 32% to 1056%.[132]

Finally, the B/C ratio, 28.6/1 for the AES project lower-bound case, says that for every $1 dollar of costs expended by NIST's AES program (1996-2017), almost $29 dollars of social benefits have been returned. For projects with the same costs, those with the highest B/C ratios would be chosen first when there is an investment budget constraint. Of 23 NIST projects evaluated for B/C, the median metric was 11, with the B/C ratios ranging from 3 to 113.[133] Because projects differ in size, the NPV metric discussed above would in practice be the one used for ranking projects, but the comparisons for the IRR and B/C ratios provide useful benchmarks and augment the understanding of the project's performance.

Considering the most conservative basis (using only the 74 respondents that provided information about their benefits from AES) for evaluating NIST's decision to invest public resources in the AES program, over the program's history, those investments have had a relatively high economic impact. On that basis alone, the impacts of NIST's efforts are considerably underestimated. A truer sense of the social returns to the AES program

[132] Ibid.
[133] Ibid.

are obtained by, first, extrapolating the benefits for an additional 95 respondents (that provided sufficient information about their activities and organizational type) to have an estimate of the benefits for all 169 (74 + 95) respondents to the economic impact survey, and, second, by extrapolating the benefits for the larger national economy.

Combining the information from the 74 survey respondents used to calculate the NPV, IRR, and B/C metrics just discussed, with the information provided by the additional 95 less complete survey responses, analogous metrics were developed for the combined group of 169 respondents. Developing the metrics for the larger group of respondents required a reconceptualization of the NPV metric. In the brief discussion of NPV above, the authors envisioned the AES program managers as standing in 1996 and looking to the future and knowing what we now know retrospectively (based on survey data) to be the NPV of the AES program, cumulating the appropriately discounted annual information about inflation-adjusted 2017 dollars. That NPV was $844,500,000.

Extrapolating this result to all 169 survey respondents and then beyond that to the larger economy requires the following perspective. Rather than looking from the initiation of the project in 1996 into to the future, envision NIST managers in 2017 looking back (after the years of costs and benefits from 1996 through 2017) at the 1996 net economic value of $844,500,000 actually achieved and asking, “If that amount had been invested and annually earned the cost of capital required of government technology investments (7%), what would be the inflation-adjusted value of that investment today in 2017?” Answering this question gives the impact of the AES program a more contemporary meaning.

The result of performing that operation on the series of cumulated *benefits* extrapolated for the 169 survey respondents finds that present value of *benefits* from today’s perspective is approximately $8.9 billion. On the other hand, the present value of NIST’s *costs* from today’s perspective is $127 million. Thus, the NPV from today’s perspective is $8,772,000,000; the B/C ratio is therefore 70.2/1; and a measure (explained in detail in Section 6.1) of the IRR for the alternative investment perspective is 31%; all are indicators of a substantial economic impact.

Extending the approach of looking back from 2017 to the larger national economy required the selection of economic sectors best represented by the 169 survey respondents. The economic sectors represented by ten or more survey respondents include the following: agriculture; construction; manufacturing; retail trade; transportation and warehousing; information; real estate rental and leasing; professional, scientific, and technical services; management services; waste management; educational services; and arts and entertainment. Looking at the present value of benefits and costs from 2017's perspective for these economic sectors finds that the present value of *benefits* rises to approximately $251 billion while the present value of NIST's *costs* from today's perspective remains the same at $127 million. Therefore, the NPV of the benefits of the AES program to the national economy from today's perspective is $250,473,200,000; the B/C ratio is roughly 1976/1; and the appropriate, alternative (explained in Section 6.1) IRR and investing proceeds at the social rate of return is 53.6%.

As substantial as these impact metrics are, they are nevertheless conservative lower bound estimates of actual economic impact for reasons explained in Section 6.2. In brief, in all cases the choice was made to interpret survey responses in the most conservative light. In other words, if the analyst had a choice between a high and low value in a response, the low value was selected.

Second, many respondents provided some useful information but not enough to directly quantify the economic benefits they enjoyed. The reasons they did not provide quantifiable impact information are numerous. Respondents' recognition of benefits and yet not being able to quantify them is a problem that has affected economic impact assessments since economists first undertook them.[134] The fact that many respondents did provided information to enable making direct impact assessments, illustrates that whatever the reasons for non-responses were, they are not binding on all respondents in roughly similar situations. Survey questions for economic impact assessments tend to require respondents' concentration and at times imagination, and the application of those qualities requires time which is in short supply among busy survey populations.

[134] See, Edwin Mansfield, et. al., "Social and Private Rates of Return from Industrial Innovations," *The Quarterly Journal of Economics,* Vol. 91, No. 2 (May 1977), pp. 221-240.

Finally, even in the case of benefits scaled to the level of the economy, a conservative choice was made to restrict benefits to only those industrial sectors represented by ten or more survey respondents.  For economic sectors with fewer than ten respondents, we know that these sectors of the economy have benefited from AES too, but we have not extrapolated benefits for them.  From the most conservative assessment of economic impact presented here to the most carefully extrapolated impacts, NIST's decision in 1996 to structure an internationally competitive search for a sufficiently strong information encryption standard was, and continues to be, an exceptional economic success.

# Appendix A. Switching Costs and the Transition to AES: The Case of Financial Industry Encryption Standards

## Introduction

At the outset of this assessment, the existence of effectively two cryptographic standards (TDES and AES) was perplexing. This case study of attempts to come to terms with it from an economic perspective.

As discussed at length in Section 2, Background, in the face of fairly dramatic changes in the cryptographic policy environment since the announcement of NIST's first encryption standard (DES) in 1976—including the commercialization and internationalization of cryptography, the looming digital revolution, and citizens' growing concern (as consumers and business owners) about the problem and costs of compromised confidentiality, integrity, and authenticity—the forces of cryptographic innovation striving to develop stronger encryption, confronted the installed base of DES-based encryption systems.

Hypothetically, NIST could have chosen to wipe the slate clean and require all Federal users to incorporate the AES algorithm in their encryption systems; however, NIST chose to accommodate agencies and suppliers facing high switching costs by slowly and incrementally raising the acceptable key strengths of TDES-based encryption systems. By effectively choosing both AES and TDES as acceptable symmetric block ciphers, NIST recognized the high switching costs that would be borne by organizations locked-in to DES-based encryption systems, and, for organizations unencumbered by significant switching costs on both the demand and supply sides of the encryption systems market, offered a path to dramatically reduced information security risk along with improved processing performance. The following sections explore the economic logic of that decision as it played out in the financial industry.

## The Financial Industry Adopts DES

NIST published DES (FIPS-46) in January 1977, and it became the standard cryptographic algorithm for the financial services industry to protect sensitive customer data. DES was adopted as the ANSI X3.32 Data Encryption Algorithm (DEA) in 1981. The banking and financial industry's standards body, ANSI's ASC X9 (hereafter X9) followed with the development of related standards for message authentication (X9.9-1994), key management (X9.17-1995), and wholesale financial message encryption (X9.23-1995).[135]

Banking automated teller machines (ATM) were largely designed to operate on DES and TDES encryption systems. In the period 1975-1997 the number of ATMs grew from approximately 4,000 to 200,000 nationally.[136] The growth in the number of ATMs reflects the growth of all manner of point-of-sale transactions (debit or credit cards) wherever they occur: gas stations, grocery stores, and restaurants to name a few. The use of bank cards in place of cash was protected by DES and TDES encryption, however as mentioned previously, serious threats arose in the 1990s challenging DES security. In 1997 and again in 1999, the RSA Security Corporation sponsored competitions that produced successful brute force attacks on DES, cracking the cipher in less than 24 hours.[137] The financial industry and the Federal Government understood these demonstrations as a harbinger that the DES life cycle (its "crypto-period") was reaching its end. The events instigated X9 to withdraw several DES-based standards. In addition, the Federal Reserve Bank, NIST, and the American Bankers Association issued recommendation letters, recommending migration from DES to Triple DES.[138]

It comes as somewhat of a surprise then to find that industry contacts consistently mention the financial sector, particularly ATM and chip card hardware, as the slowest sector to make the switch to AES. Why? From an economic perspective, the answer in a nutshell is "switching costs." This appears to be the case for the financial industry, and it is suspected to be the case for other sectors where TDES maintained its prevalence. As discussed in Section 5, Survey Findings, many private sector consumers of AES did not switch from TDES until 2010 or later. For the financial sector, the massive network of encrypted hardware and software assets built up over two decades were geared to DES. Like the momentum that requires a big ship to turn slowly in a wide arch, so the time and

[135] *Technical Report: Migration from DES* (TR-37 2009), Accredited Standards Committee X9, Inc.
[136] Leech and Chinworth, op. cit., p. 26.
[137] For the 1997 event a $250,000 computer built by the Electronic Frontier Foundation (EFF) decrypted a DES-encoded message in 56 hours. In 1999 this was improved to 22 hours through a combination of 100,000 networked PCs and the EFF machine. Susan Landau, "Standing the Test of Time: The Data Encryption Standard," *Notices of the AMS*, Vol. 47, No.3, March 2000, pp. 341-349.
[138] Accredited Standards Committee X9, op. cit., p. xv.

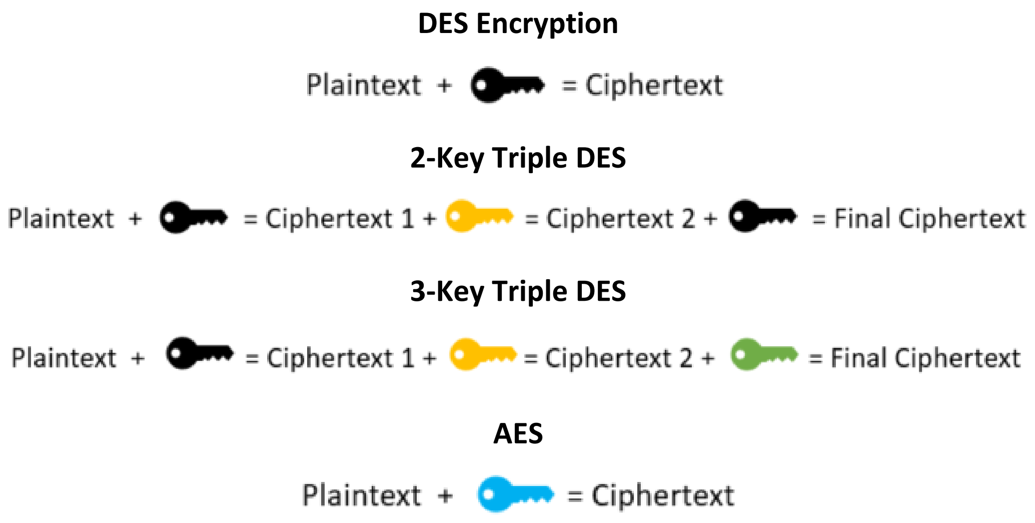
costs of switching from TDES to AES requires a two-standards solution until 2030**.** In terms of economic impact, the slow pace of adoption in some sectors pushes the beneficial effects of AES to a later, and thus shorter, period in the assessment timeframe.

## Transitioning from DES to TDES to AES

Although TDES is essentially running DES encryption multiple times, a transition from DES to TDES is technically complex, involving changes in the way the algorithm works and in its modes of operation. That complexity could be amplified depending on, for example, the cryptographic schemes for key management employed by user organizations.[139] It is helpful to understand how cryptographic keys are employed in DES and TDES and how this contrasts with AES.

Figure A-1 uses colors to illustrate how keys are used in each algorithm; it does not delve into the fundamental differences between DES/TDES and AES encryption rounds and permutations. DES operates with one 56-bit key in a very straightforward manner. Triple DES uses either 2 or 3 56-bit keys and has multiple encryption rounds. 2-Key TDES effectively achieves a 112-bit key strength, while 3-Key TDES holds 168-bit key strength. Finally, AES uses a single 128, 192, or 256-bit key.

*Figure A-1. The "Keys" to High Switching Costs*


DES Encryption
Plaintext + = Ciphertext
2-Key Triple DES
Plaintext + = Ciphertext 1 + = Ciphertext 2 + = Final Ciphertext
3-Key Triple DES
Plaintext + = Ciphertext 1 + = Ciphertext 2 + = Final Ciphertext
AES
Plaintext + = Ciphertext

[139] Ibid. Four modes of operation are discussed in the X9 technical report: Triple DEA Electronic Code Book (TECB), Triple DEA Cipher Block Chaining (TCBC), Triple DEA Cipher Feed Back (TCFB), and Triple DEA Output Feed Back (TOFB). Three key management schemes are also described: Fixed Transaction Key Method, Master Key/Session Key, and Derived Unique Key Per Transaction (DUKPT).

Due to its underlying design, not strictly related to key size, AES enables a more secure and efficient encryption process in software implementations.[140] In a simple laptop application, encrypting approximately 1000-byte blocks of plaintext, 3-Key TDES runs approximately three times slower than DES, which is not surprising given 3-Key TDES runs the DES algorithm three times. AES-128 runs six times faster than 3-Key TDES.[141]

By all accounts, the overall enterprise of converting from DES to TDES was a gargantuan task. A 2009 X9 report worried that, "there are still implementers who have not migrated [from DES]."[142] According to an industry representative, the transition from single DES to TDES involved a "hefty expense" for the industry:

> The key size [effectively] doubled [or tripled], so every application and device involved in the message flow had to be addressed. Hardware where a PIN is entered (ATM or POS) or translated (bank, processor, network, and issuer hardware security module) had to be upgraded and every piece of the software that communicated in or with those devices had to support longer key field in the message and differentiate between the key types. Any database where keys are stored had to support both old and new as well.[143]

An industry observer, reporting in 2008, estimated the burden on ATM operators of complying with TDES would be thousands to millions of dollars in ATM fleet upgrades, depending on fleet size. In 2005, a large independent ATM supplier estimated that TDES upgrades would take "a few years" and had budgeted $25 million in 2006 for that purpose. In most cases, upgrading machines required new encrypting PIN pads, and software and firmware upgrades to handle effectively longer encryption keys. In 2008 estimates of TDES upgrade costs were between $700 and $2,000 per machine.[144]

[140] According to one assessment, TDES takes three times as much CPU power compared with its DES predecessor. The authors of the assessment regard this as a "significant performance hit." Hamdan O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors," *Journal of Computing*, Vol. 2, Issue 3, March 2010, pp. 2151-9617. <HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/>

[141] Personal communication with Eric Burger, May 8, 2018.

[142] Ibid., p. 22.

[143] Personal communications with an X9-affiliated financial industry encryption systems expert, April 29 – May 2, 2018. (The individual's name is withheld as a condition of several email exchanges.)

[144] Gary Wollenhaupt, "Triple DES: Too high to comply?," *ATM Marketplace,* July 9, 2008. <https://www.atmmarketplace.com/articles/triple-des-too-high-to-comply/>

### Why Was TDES Retained?

First and foremost, TDES has been retained because it provided, and continues to provide, information security. Over time, the 2-Key TDES option was abandoned (disallowed by NIST after December 31, 2010). In 2008, some weaknesses in 3-Key TDES were exposed having to do with the encryption of a large number of blocks of plaintext. That year X9 withdrew its TDES Modes of Operation standard (X9.52-1998) and replaced it with a NIST special publication that recognized and addressed the problem. In 2017 that same special publication was revised and made additional adjustments to the secure threshold for the number of plaintext blocks TDES could be used on.[145] The announcement advised all TDES users to migrate to AES as soon as possible.[146]

From an economic perspective, another important reason for the existence of two encryption standards is the high cost of transitioning to the fundamentally different AES algorithm. A well-informed industry participant suggested that the transition from DES to TDES can serve as a model of the complexities and scale of the problem of transitioning to AES. "The pain of the DES-to-TDES upgrade" provided lessons learned; for example, if the difference between DES and TDES in effective key size caused trouble and expense, the transition from TDES to AES entails two entirely different algorithms, "not a matter of a tweak here and there."[147] So it stands to reason that the switching costs for organizations substantially invested in TDES encrypted systems have been considerable as they proceed to transition to AES.

The issues involved are discussed today under the rubric of "cryptographic agility:"

> Cryptographic agility refers to how easy it is to evolve or replace the hardware, software, or entire information technology (IT) systems being

[145] Elaine Barker and Nicky Mouha, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, NIST Special Publication 800-67, Revision 2, November 2017.
[146] https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea
[147] Personal communication with X9 expert, op. cit.

> used to implement cryptographic algorithms or protocols (and, in particular, whether the resulting systems remain "interoperable").[148]

A participant in a recent workshop on cryptographic agility, sponsored by the National Academies of Sciences, Engineering, and Medicine, opined that,

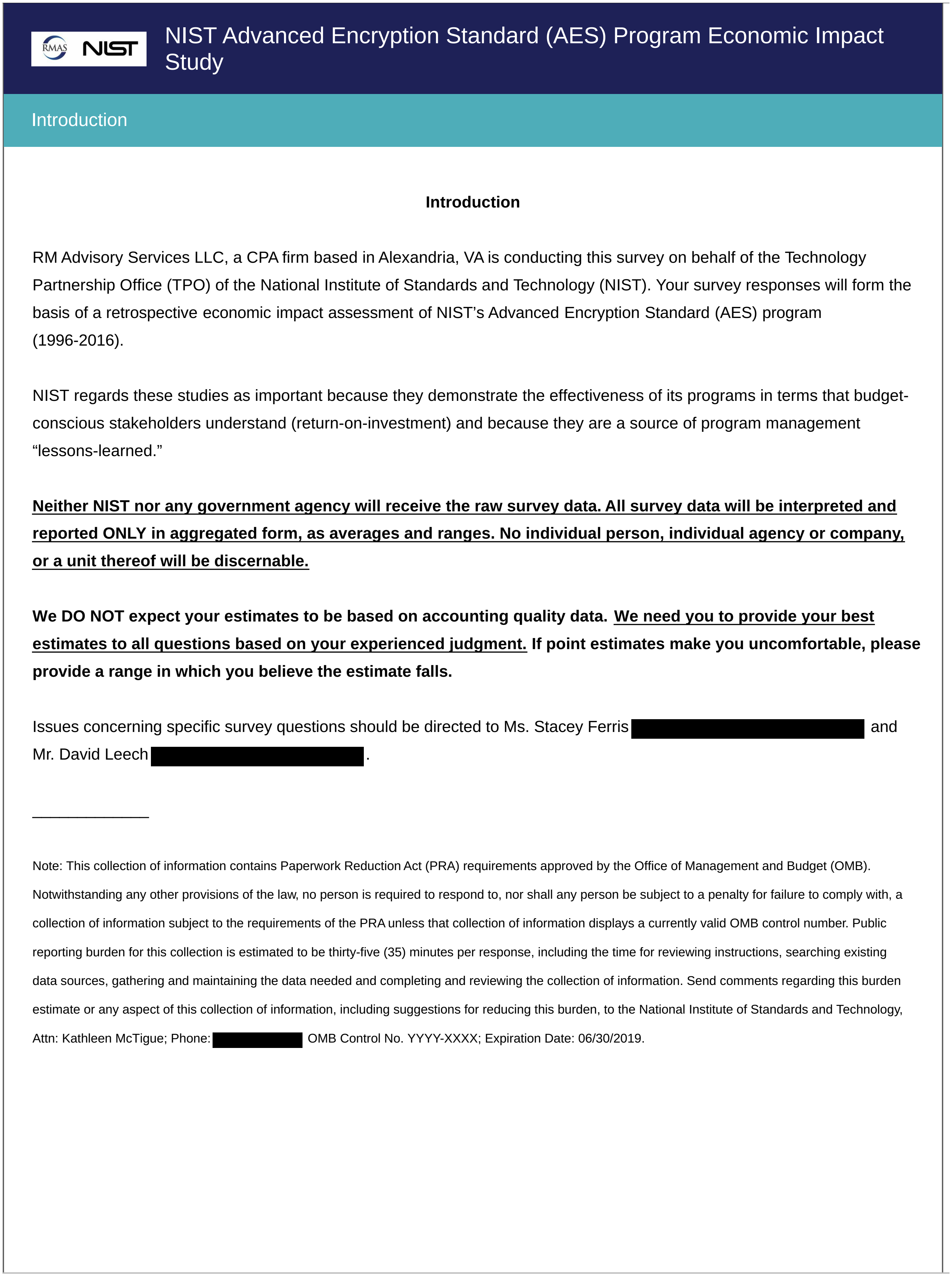
> [R]eplacing a system completely takes a long time because it requires an enormous amount of work... completely replacing a widely deployed system would take at least three years, assuming that there is already a well-tested replacement system ready for deployment, and ten years or more if a new cryptographic approach had to be developed from scratch starting at the time of the discovery of the vulnerability in the old system.[149]

Given the continued security strength of 3-Key TDES, and at the risk of projecting a current understanding onto those anticipating TDES and its eventual replacement by AES in the late 1990s, the perception that transitioning to a new standard "from scratch" was very expensive and could take ten years to develop and deploy would seem to explain why X9 and much of the financial industry stayed the course with TDES, even in the face of a demonstrably vulnerable DES, and with the AES competition underway.  History demonstrates that developing the AES standard took significantly less than ten years, only four years "from scratch," and moreover, that deploying products with AES was achievable within months for prepared organizations. Hence, there have been two symmetric block cipher encryption standards since 2001.

[148] *Cryptographic Agility and Interoperability: Proceedings of a Workshop Forum on Cyber Resilience Workshop Series,* Washington, DC: The National Academies Press, 2017, p. 2.
[149] Ibid., p. 8. These views were expressed by Bob Blakley, CitiGroup, Inc., presumably representing views held by other members of the financial services community.

# Appendix B. AES program Economic Impacts Survey Instrument

The following pages contain the survey instrument as it was distributed on the Survey Monkey Research.net platform to the three groups of respondents.  Note that the designation in the light blue bar under the heading denotes whether the questions are for group 1 “Public Sector Consumer", group 2 “Private Sector Consumer", or group 3 “Cryptographic Modules/Integrators".  These groups and the purpose of various survey questions are described in detail in Chapter 5.



# NIST Advanced Encryption Standard (AES) Program Economic Impact Study

## Introduction

### Introduction

RM Advisory Services LLC, a CPA firm based in Alexandria, VA is conducting this survey on behalf of the Technology Partnership Office (TPO) of the National Institute of Standards and Technology (NIST). Your survey responses will form the basis of a retrospective economic impact assessment of NIST's Advanced Encryption Standard (AES) program (1996-2016).

NIST regards these studies as important because they demonstrate the effectiveness of its programs in terms that budget-conscious stakeholders understand (return-on-investment) and because they are a source of program management "lessons-learned."

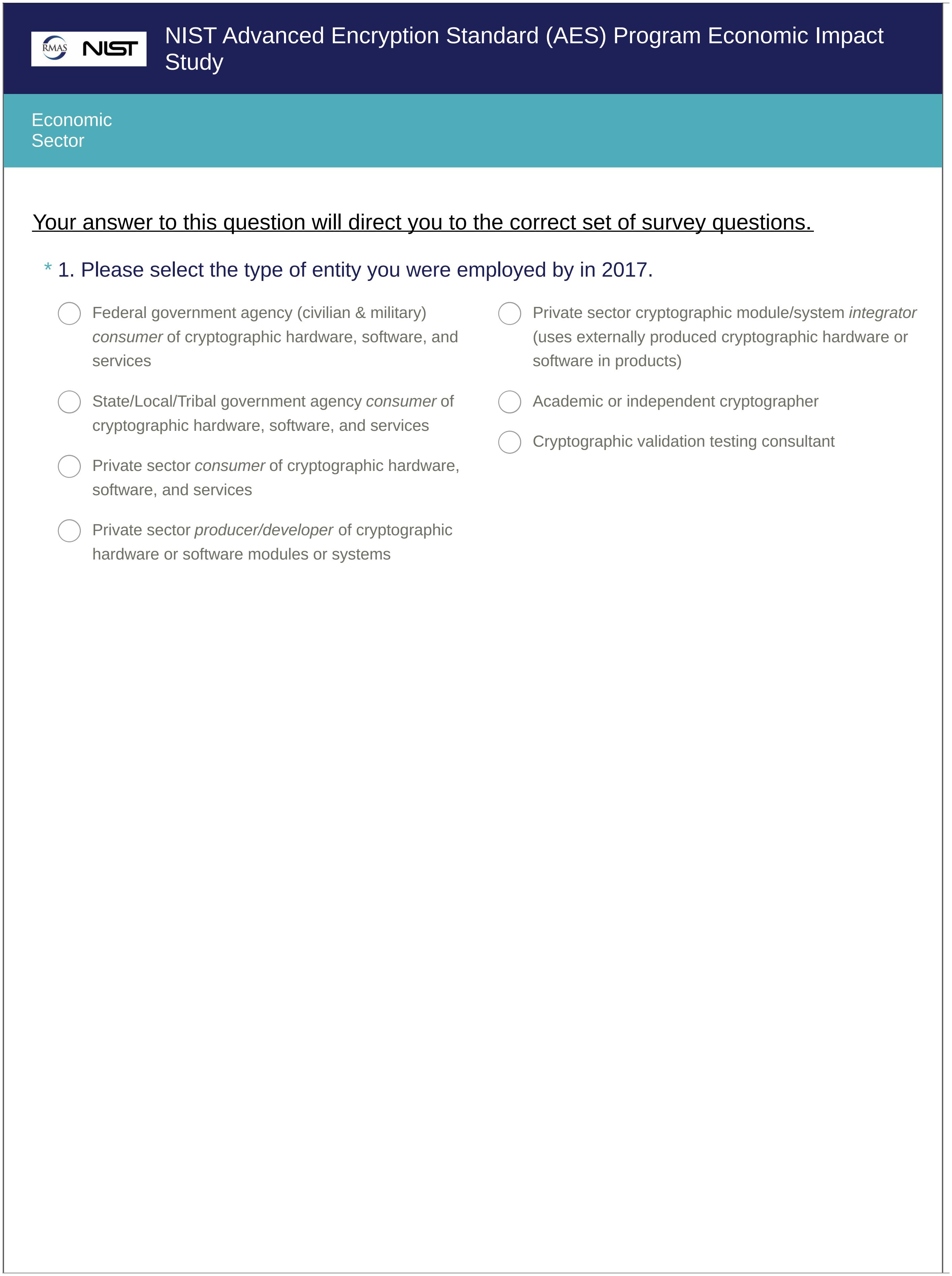
**Neither NIST nor any government agency will receive the raw survey data. All survey data will be interpreted and reported ONLY in aggregated form, as averages and ranges. No individual person, individual agency or company, or a unit thereof will be discernable.**

**We DO NOT expect your estimates to be based on accounting quality data. We need you to provide your best estimates to all questions based on your experienced judgment. If point estimates make you uncomfortable, please provide a range in which you believe the estimate falls.**

Issues concerning specific survey questions should be directed to Ms. Stacey Ferris [redacted] and Mr. David Leech [redacted].

---

Note: This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be thirty-five (35) minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Institute of Standards and Technology, Attn: Kathleen McTigue; Phone: [redacted] OMB Control No. YYYY-XXXX; Expiration Date: 06/30/2019.



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Economic Sector

Your answer to this question will direct you to the correct set of survey questions.

* 1. Please select the type of entity you were employed by in 2017.

○ Federal government agency (civilian & military) *consumer* of cryptographic hardware, software, and services

○ State/Local/Tribal government agency *consumer* of cryptographic hardware, software, and services

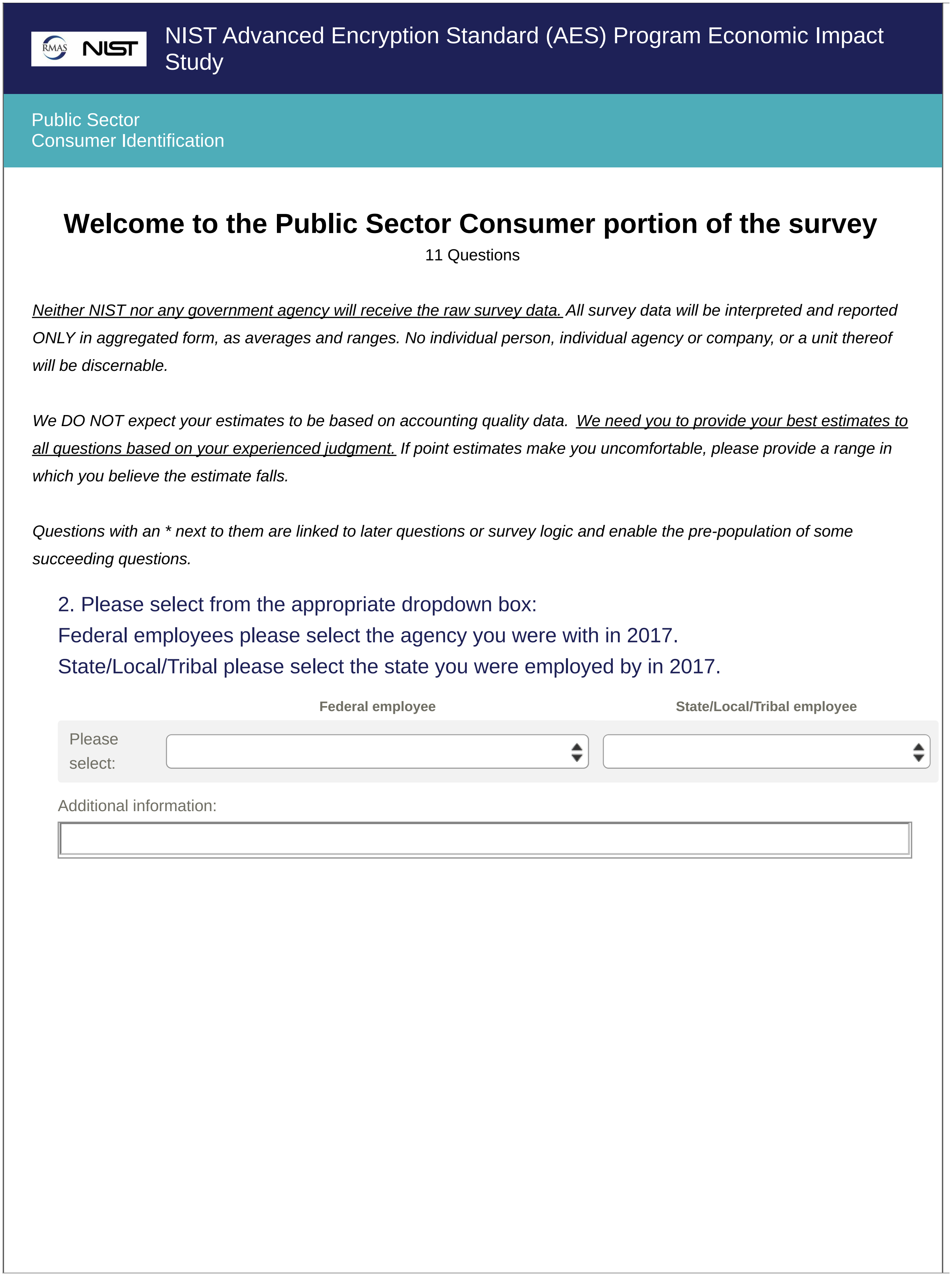
○ Private sector *consumer* of cryptographic hardware, software, and services

○ Private sector *producer/developer* of cryptographic hardware or software modules or systems

○ Private sector cryptographic module/system *integrator* (uses externally produced cryptographic hardware or software in products)

○ Academic or independent cryptographer

○ Cryptographic validation testing consultant



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Public Sector
Consumer Identification

## Welcome to the Public Sector Consumer portion of the survey

11 Questions

*Neither NIST nor any government agency will receive the raw survey data. All survey data will be interpreted and reported ONLY in aggregated form, as averages and ranges. No individual person, individual agency or company, or a unit thereof will be discernable.*

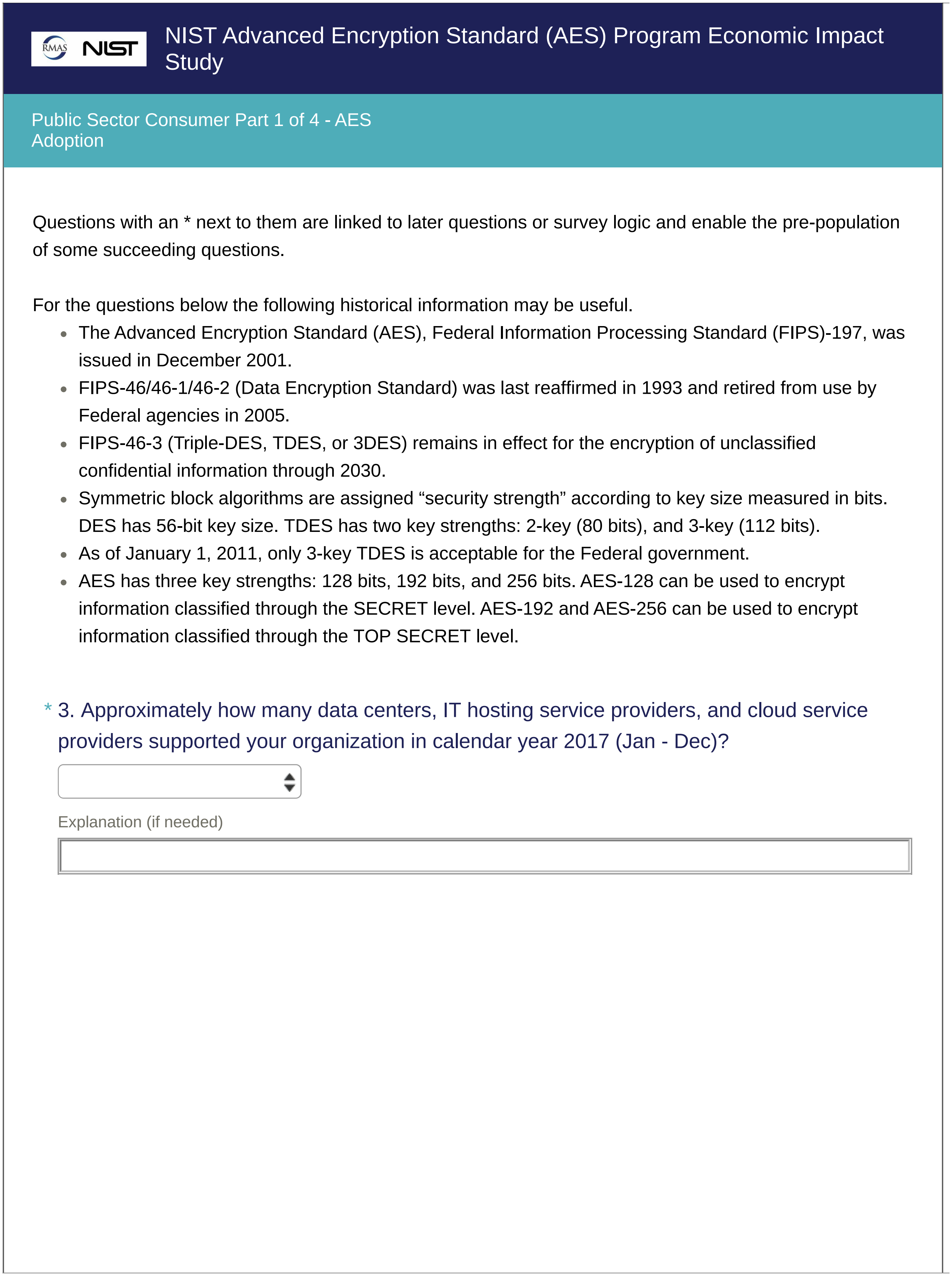
*We DO NOT expect your estimates to be based on accounting quality data. We need you to provide your best estimates to all questions based on your experienced judgment. If point estimates make you uncomfortable, please provide a range in which you believe the estimate falls.*

*Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.*

2. Please select from the appropriate dropdown box:
Federal employees please select the agency you were with in 2017.
State/Local/Tribal please select the state you were employed by in 2017.

| | Federal employee | State/Local/Tribal employee |
|---|---|---|
| Please select: | | |

Additional information:



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Public Sector Consumer Part 1 of 4 - AES Adoption

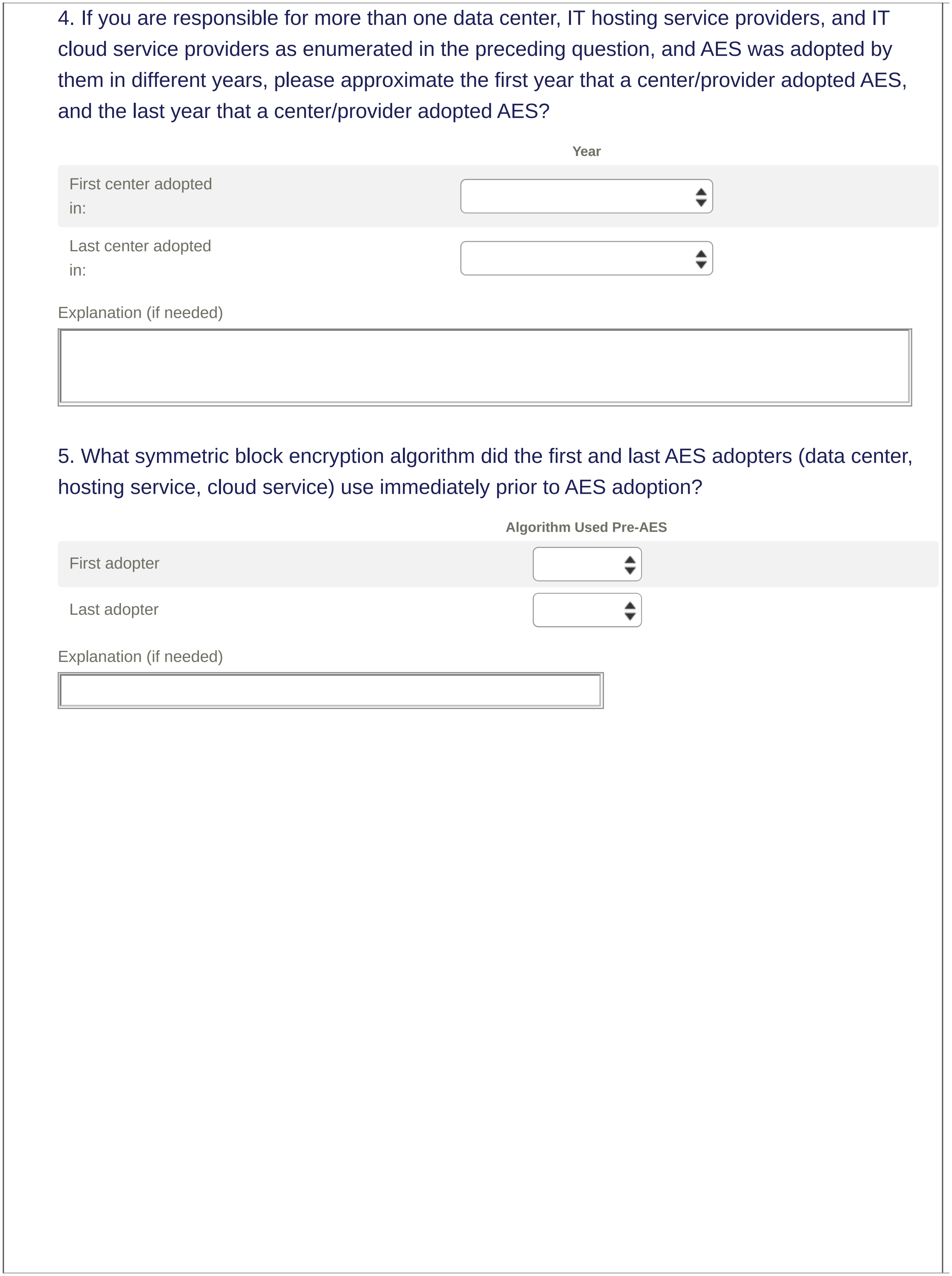
Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.

For the questions below the following historical information may be useful.

- The Advanced Encryption Standard (AES), Federal Information Processing Standard (FIPS)-197, was issued in December 2001.
- FIPS-46/46-1/46-2 (Data Encryption Standard) was last reaffirmed in 1993 and retired from use by Federal agencies in 2005.
- FIPS-46-3 (Triple-DES, TDES, or 3DES) remains in effect for the encryption of unclassified confidential information through 2030.
- Symmetric block algorithms are assigned “security strength” according to key size measured in bits. DES has 56-bit key size. TDES has two key strengths: 2-key (80 bits), and 3-key (112 bits).
- As of January 1, 2011, only 3-key TDES is acceptable for the Federal government.
- AES has three key strengths: 128 bits, 192 bits, and 256 bits. AES-128 can be used to encrypt information classified through the SECRET level. AES-192 and AES-256 can be used to encrypt information classified through the TOP SECRET level.

* 3. Approximately how many data centers, IT hosting service providers, and cloud service providers supported your organization in calendar year 2017 (Jan - Dec)?

Explanation (if needed)



4. If you are responsible for more than one data center, IT hosting service providers, and IT cloud service providers as enumerated in the preceding question, and AES was adopted by them in different years, please approximate the first year that a center/provider adopted AES, and the last year that a center/provider adopted AES?

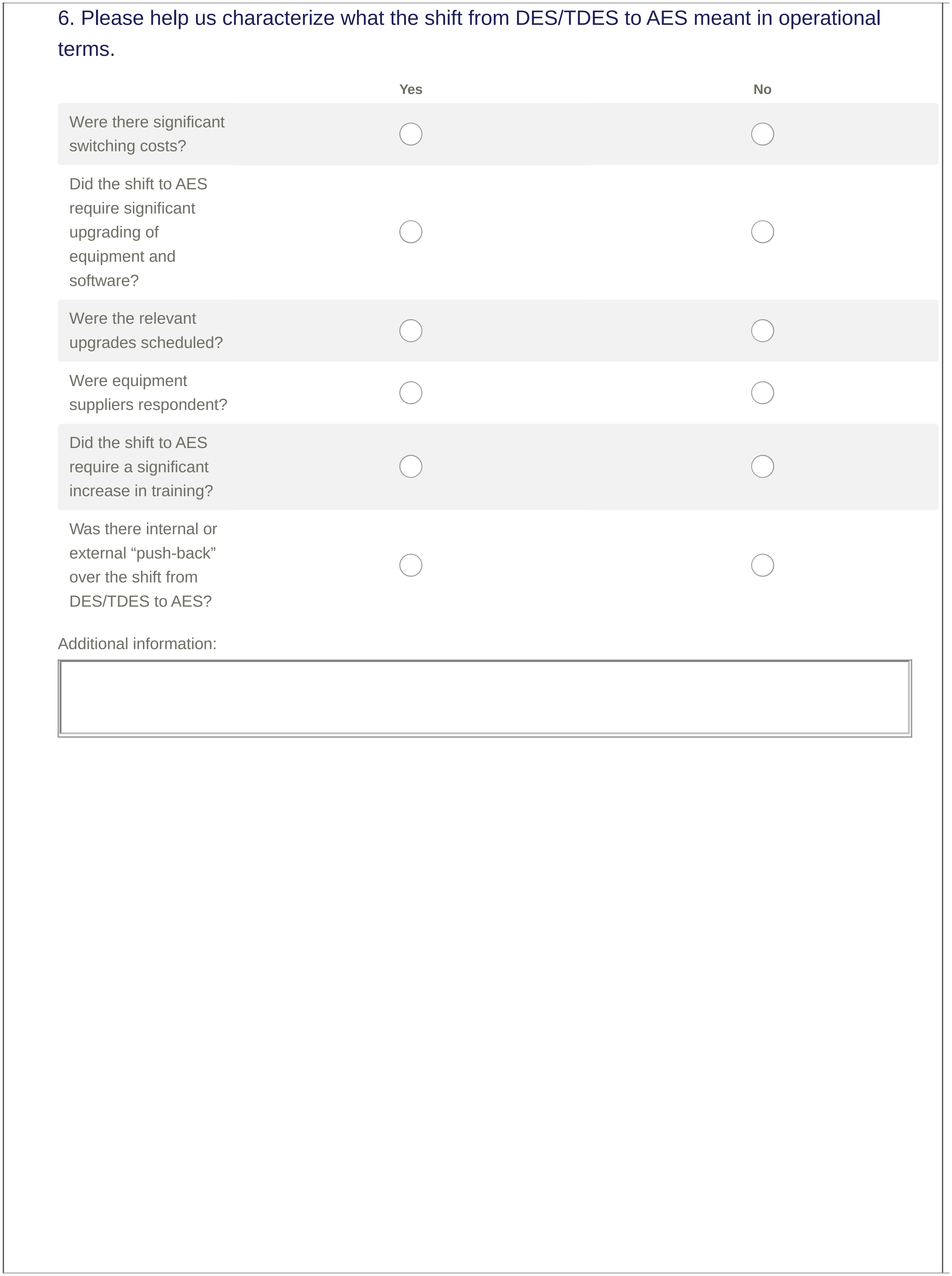
| | Year |
|---|---|
| First center adopted in: | |
| Last center adopted in: | |

Explanation (if needed)

5. What symmetric block encryption algorithm did the first and last AES adopters (data center, hosting service, cloud service) use immediately prior to AES adoption?

| | Algorithm Used Pre-AES |
|---|---|
| First adopter | |
| Last adopter | |

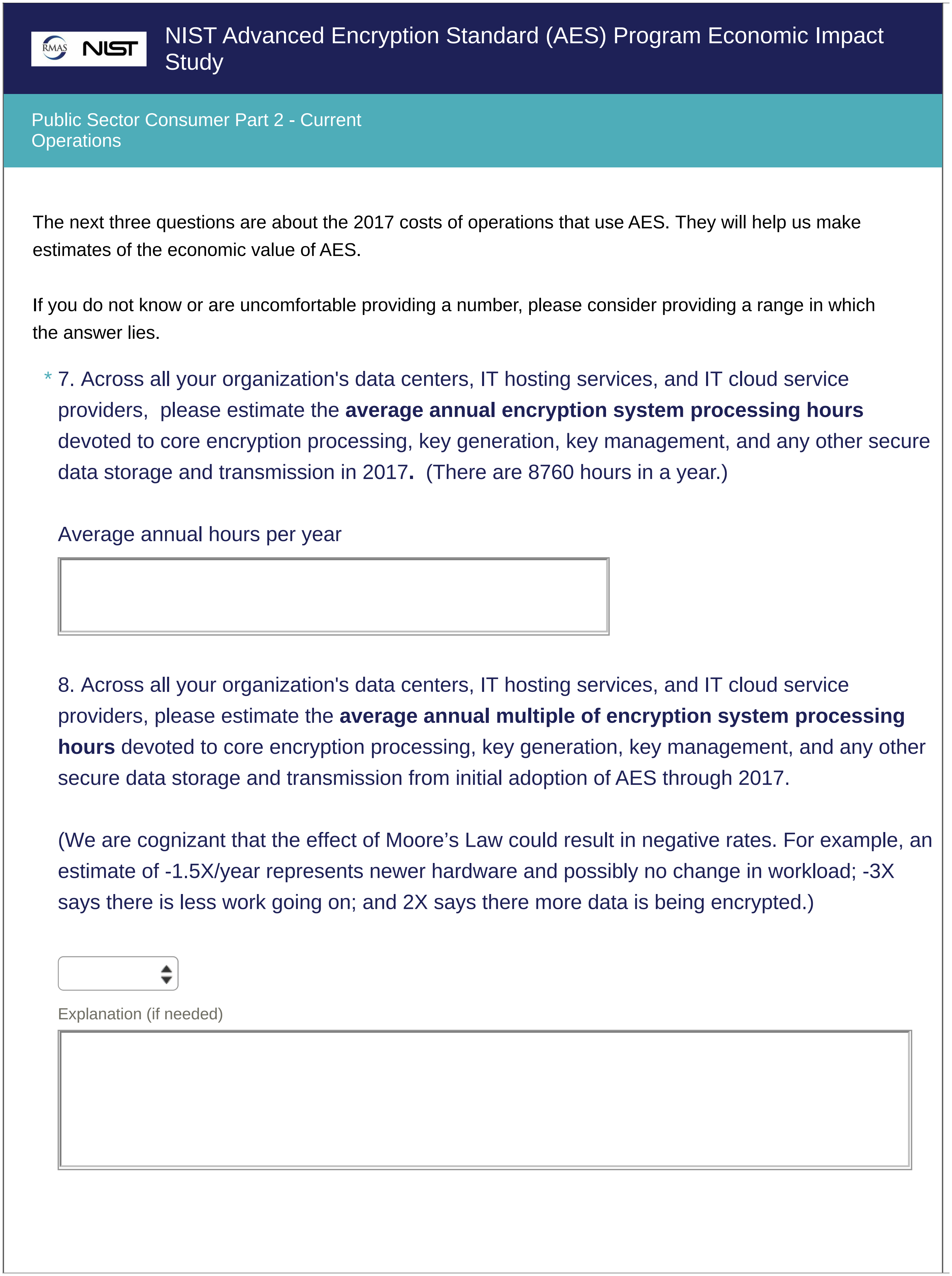
Explanation (if needed)



6. Please help us characterize what the shift from DES/TDES to AES meant in operational terms.

| | Yes | No |
|---|---|---|
| Were there significant switching costs? | ○ | ○ |
| Did the shift to AES require significant upgrading of equipment and software? | ○ | ○ |
| Were the relevant upgrades scheduled? | ○ | ○ |
| Were equipment suppliers respondent? | ○ | ○ |
| Did the shift to AES require a significant increase in training? | ○ | ○ |
| Was there internal or external “push-back” over the shift from DES/TDES to AES? | ○ | ○ |

Additional information:



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Public Sector Consumer Part 2 - Current Operations

The next three questions are about the 2017 costs of operations that use AES. They will help us make estimates of the economic value of AES.

If you do not know or are uncomfortable providing a number, please consider providing a range in which the answer lies.

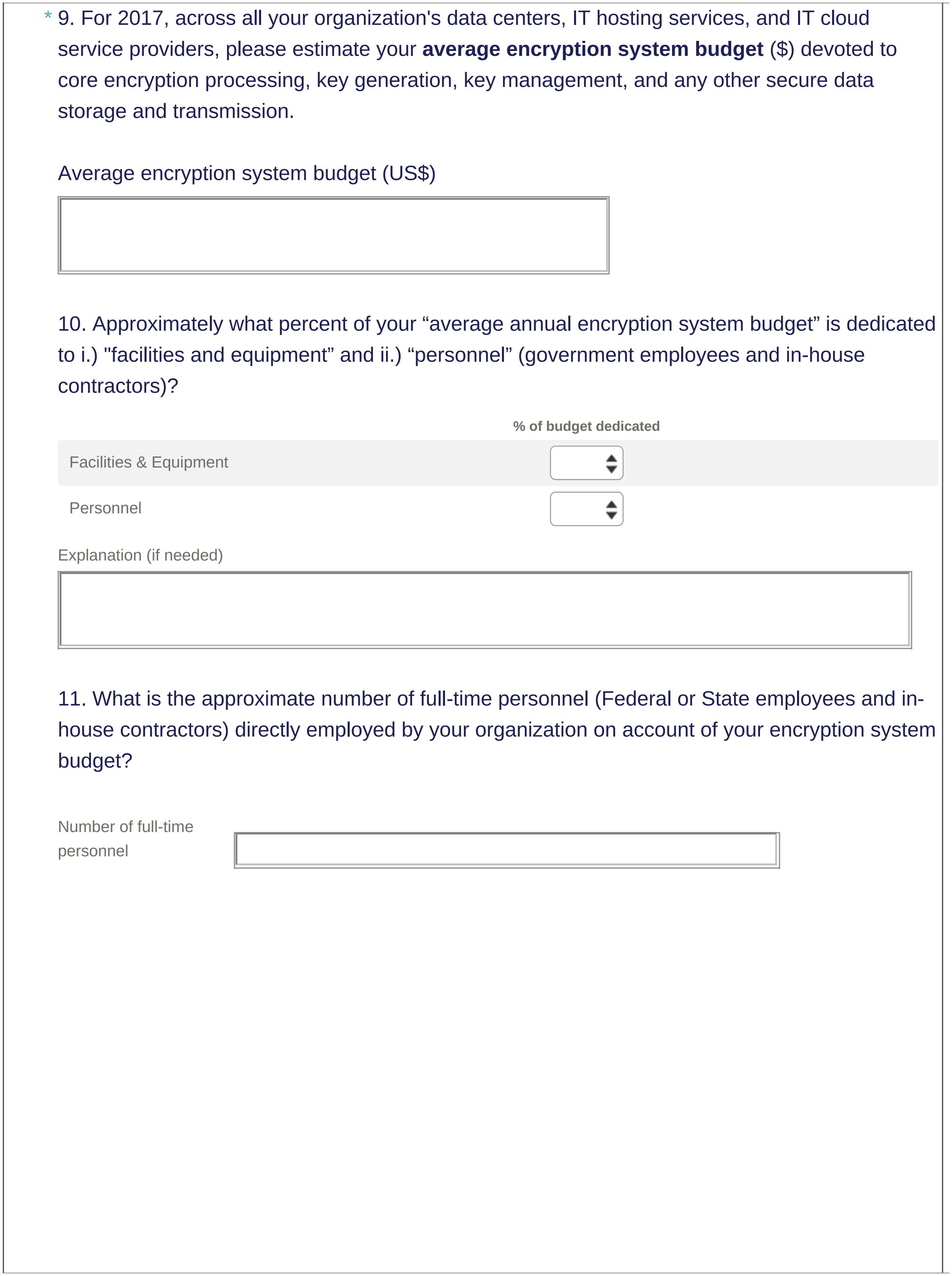
* 7. Across all your organization's data centers, IT hosting services, and IT cloud service providers, please estimate the **average annual encryption system processing hours** devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission in 2017**.** (There are 8760 hours in a year.)

Average annual hours per year

8. Across all your organization's data centers, IT hosting services, and IT cloud service providers, please estimate the **average annual multiple of encryption system processing hours** devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission from initial adoption of AES through 2017.

(We are cognizant that the effect of Moore’s Law could result in negative rates. For example, an estimate of -1.5X/year represents newer hardware and possibly no change in workload; -3X says there is less work going on; and 2X says there more data is being encrypted.)

Explanation (if needed)



* 9. For 2017, across all your organization's data centers, IT hosting services, and IT cloud service providers, please estimate your **average encryption system budget** ($) devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission.

Average encryption system budget (US$)

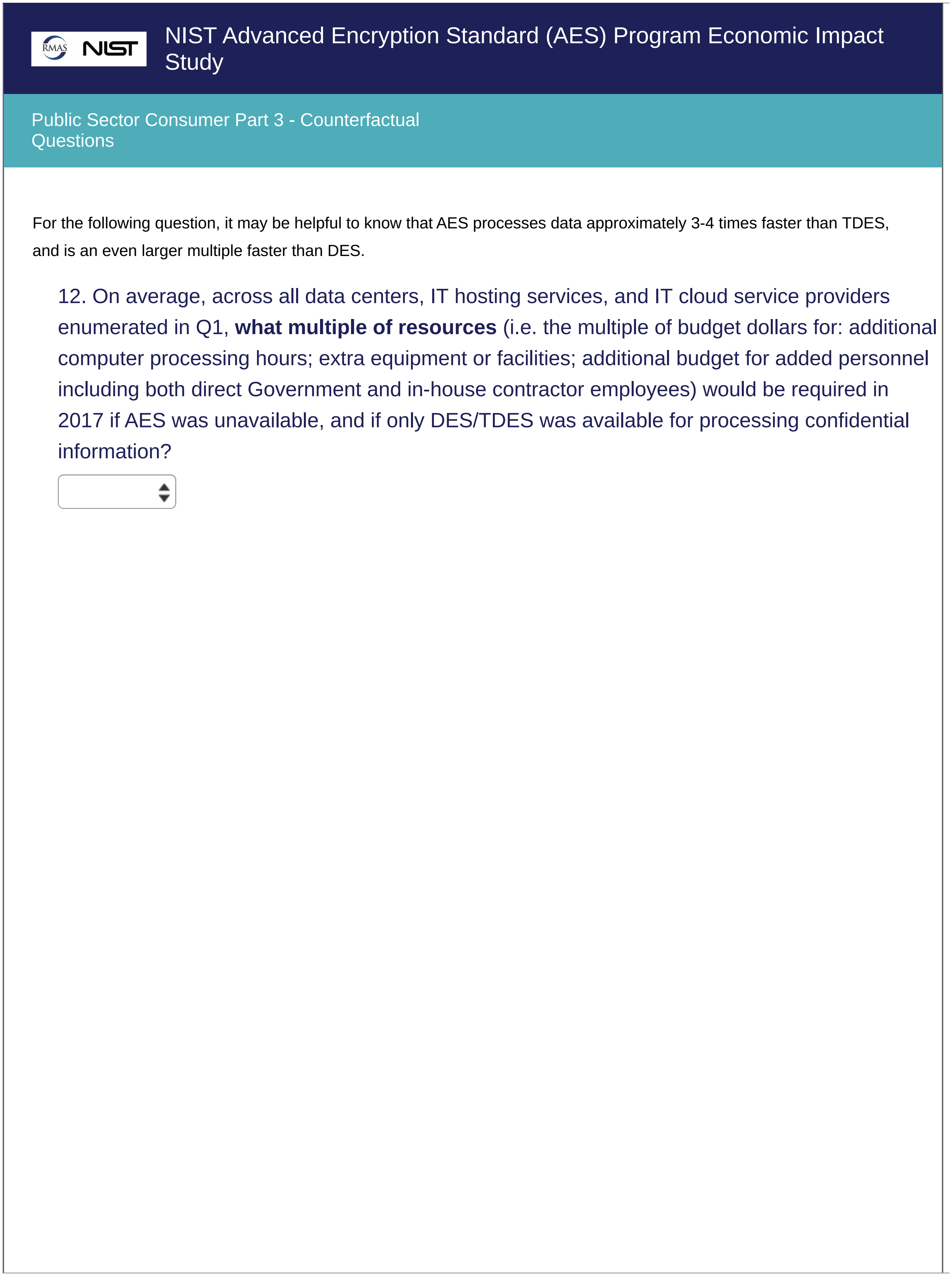
10. Approximately what percent of your “average annual encryption system budget” is dedicated to i.) "facilities and equipment” and ii.) “personnel” (government employees and in-house contractors)?

| | % of budget dedicated |
|---|---|
| Facilities & Equipment | |
| Personnel | |

Explanation (if needed)

11. What is the approximate number of full-time personnel (Federal or State employees and in-house contractors) directly employed by your organization on account of your encryption system budget?

Number of full-time personnel



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Public Sector Consumer Part 3 - Counterfactual Questions

For the following question, it may be helpful to know that AES processes data approximately 3-4 times faster than TDES, and is an even larger multiple faster than DES.

12. On average, across all data centers, IT hosting services, and IT cloud service providers enumerated in Q1, **what multiple of resources** (i.e. the multiple of budget dollars for: additional computer processing hours; extra equipment or facilities; additional budget for added personnel including both direct Government and in-house contractor employees) would be required in 2017 if AES was unavailable, and if only DES/TDES was available for processing confidential information?

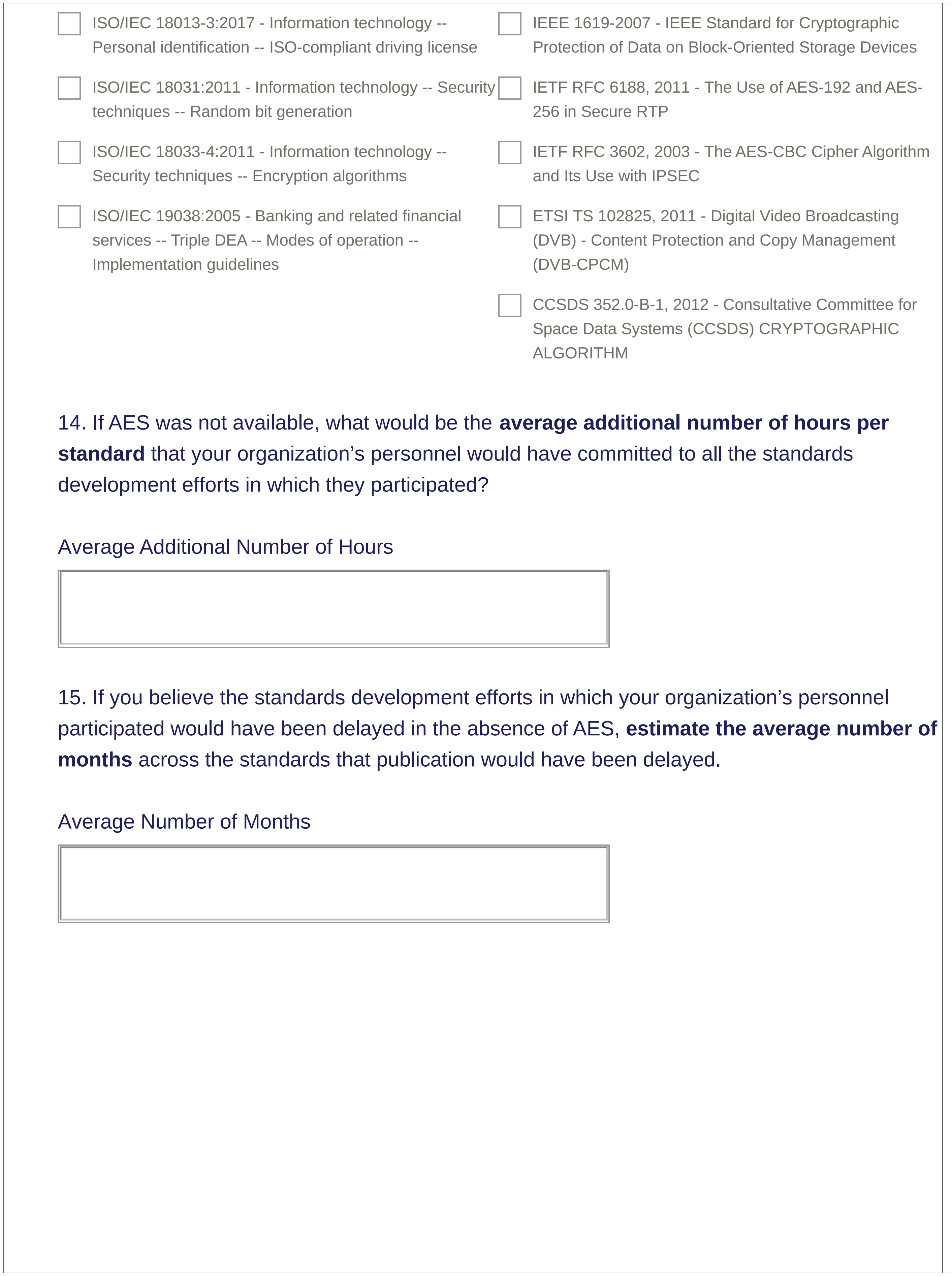
# NIST Advanced Encryption Standard (AES) Program Economic Impact Study

## Public Sector Consumer Part 4 - Standards Development

The following questions refer to the diffusion of strong encryption technology as represented in the proliferation of international standards for which AES is regarded as “indispensible” (i.e., included as a normative reference).

### 13. Select all of the following consensus standards development efforts (and/or their U.S. counterparts) in which members of your organization participated.
### This list includes standards from ISO, IEEE, IETF, and CCSDS.

- □ ISO/IEC 9564:2014 - Financial services — Personal Identification Number (PIN) management and security
- □ ISO/IEC 9797:2011 - Information technology -- Security techniques -- Message Authentication Codes (MACs)
- □ ISO/IEC 10116:2017 - Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
- □ ISO/IEC 11568:2012 - Financial services -- Key management (retail)
- □ ISO/IEC 11889:2015 - Information technology -- Trusted Platform Module
- □ ISO/IEC 13141:2015 - Electronic fee collection -- Localisation augmentation communication for autonomous systems
- □ ISO/IEC 13157-2:2016 - Information technology -- Telecommunications and information exchange between systems -- NFC Security
- □ ISO/TR 13569:2005 - Financial services -- Information security guidelines
- □ ISO/IEC 14543:2010 - Information technology -- Home electronic system (HES) architecture
- □ ISO/IEC 15764:2004 - Road vehicles -- Extended data link security
- □ ISO/IEC 16504:2011 - Information technology -- Telecommunications and information exchange between systems -- MAC and PHY for operation in TV white space
- □ ISO/IEC 19772:2009 - Information technology -- Security techniques -- Authenticated encryption
- □ ISO/IEC 23001:2015 - Information technology -- MPEG systems technologies
- □ ISO/IEC DIS 23009:2013 - Information technology -- Dynamic adaptive streaming over HTTP (DASH)
- □ ISO/TS 24534:2011 - Road transport and Traffic Telematics - Automatic Vehicle and Equipment Identification - Electronic Registration Identification (ERI) for Vehicles
- □ ISO/IEC 24767:2009 - Information technology -- Home network security
- □ ISO/IEC 24771:2014 - Information technology -- Telecommunications and information exchange between systems -- MAC/PHY standard for ad hoc wireless network to support QoS in an industrial work environment
- □ ISO/IEC 25185:2016 - Identification cards -- Integrated circuit card authentication protocols
- □ ISO/IEC 26430:2008 - Digital cinema (D-cinema) operations
- □ IEEE 802.1 AE: 2006 - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
- □ IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages



□ ISO/IEC 18013-3:2017 - Information technology -- Personal identification -- ISO-compliant driving license

□ ISO/IEC 18031:2011 - Information technology -- Security techniques -- Random bit generation

□ ISO/IEC 18033-4:2011 - Information technology -- Security techniques -- Encryption algorithms

□ ISO/IEC 19038:2005 - Banking and related financial services -- Triple DEA -- Modes of operation -- Implementation guidelines

□ IEEE 1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

□ IETF RFC 6188, 2011 - The Use of AES-192 and AES-256 in Secure RTP

□ IETF RFC 3602, 2003 - The AES-CBC Cipher Algorithm and Its Use with IPSEC

□ ETSI TS 102825, 2011 - Digital Video Broadcasting (DVB) - Content Protection and Copy Management (DVB-CPCM)

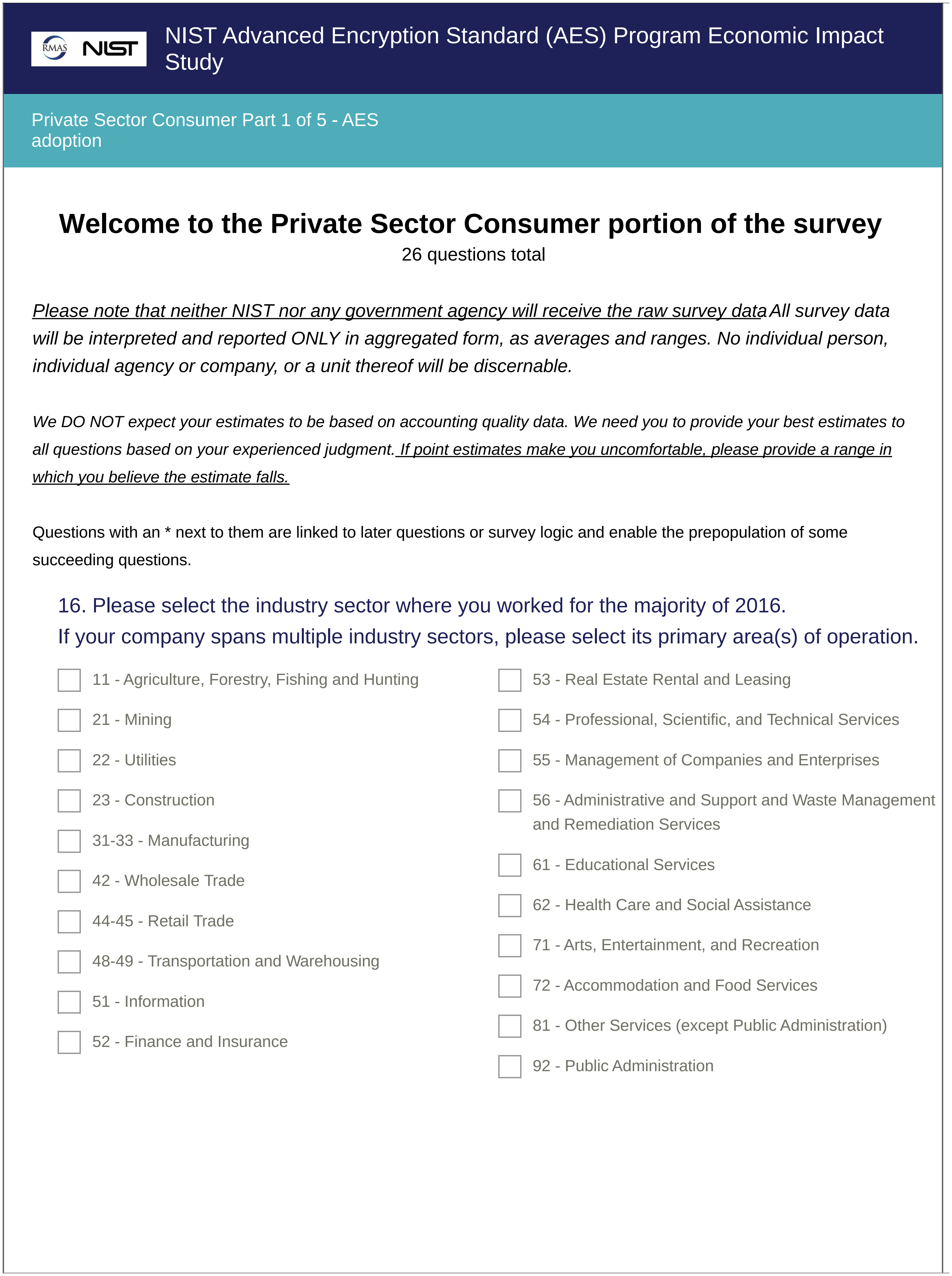
□ CCSDS 352.0-B-1, 2012 - Consultative Committee for Space Data Systems (CCSDS) CRYPTOGRAPHIC ALGORITHM

14. If AES was not available, what would be the **average additional number of hours per standard** that your organization's personnel would have committed to all the standards development efforts in which they participated?

Average Additional Number of Hours

15. If you believe the standards development efforts in which your organization's personnel participated would have been delayed in the absence of AES, **estimate the average number of months** across the standards that publication would have been delayed.

Average Number of Months



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Private Sector Consumer Part 1 of 5 - AES adoption

## Welcome to the Private Sector Consumer portion of the survey

26 questions total

*Please note that neither NIST nor any government agency will receive the raw survey data All survey data will be interpreted and reported ONLY in aggregated form, as averages and ranges. No individual person, individual agency or company, or a unit thereof will be discernable.*

*We DO NOT expect your estimates to be based on accounting quality data. We need you to provide your best estimates to all questions based on your experienced judgment. If point estimates make you uncomfortable, please provide a range in which you believe the estimate falls.*

Questions with an * next to them are linked to later questions or survey logic and enable the prepopulation of some succeeding questions.

### 16. Please select the industry sector where you worked for the majority of 2016. If your company spans multiple industry sectors, please select its primary area(s) of operation.

□ 11 - Agriculture, Forestry, Fishing and Hunting

□ 21 - Mining

□ 22 - Utilities

□ 23 - Construction

□ 31-33 - Manufacturing

□ 42 - Wholesale Trade

□ 44-45 - Retail Trade

□ 48-49 - Transportation and Warehousing

□ 51 - Information

□ 52 - Finance and Insurance

□ 53 - Real Estate Rental and Leasing

□ 54 - Professional, Scientific, and Technical Services

□ 55 - Management of Companies and Enterprises

□ 56 - Administrative and Support and Waste Management and Remediation Services

□ 61 - Educational Services

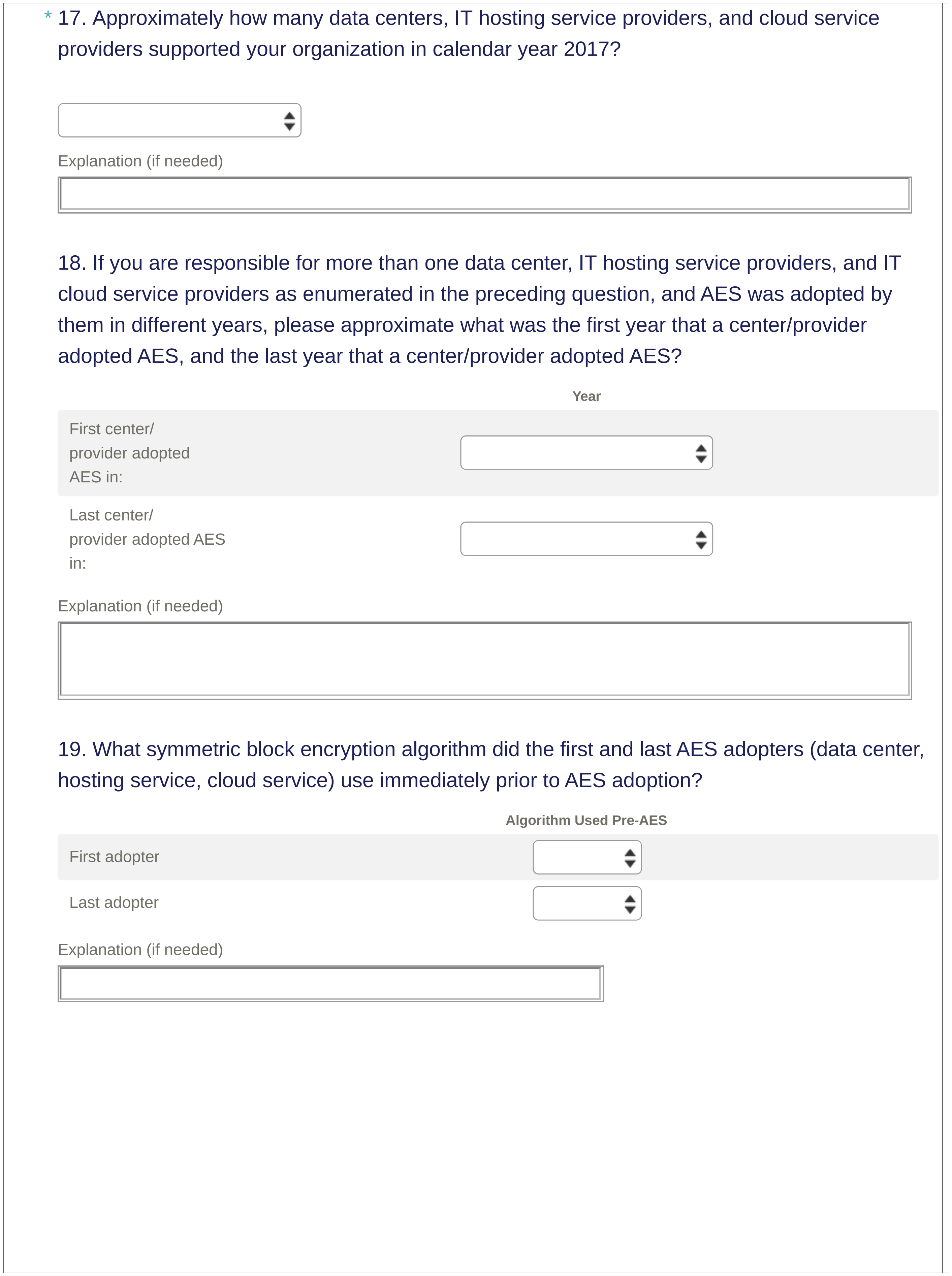
□ 62 - Health Care and Social Assistance

□ 71 - Arts, Entertainment, and Recreation

□ 72 - Accommodation and Food Services

□ 81 - Other Services (except Public Administration)

□ 92 - Public Administration



* 17. Approximately how many data centers, IT hosting service providers, and cloud service providers supported your organization in calendar year 2017?

Explanation (if needed)

18. If you are responsible for more than one data center, IT hosting service providers, and IT cloud service providers as enumerated in the preceding question, and AES was adopted by them in different years, please approximate what was the first year that a center/provider adopted AES, and the last year that a center/provider adopted AES?

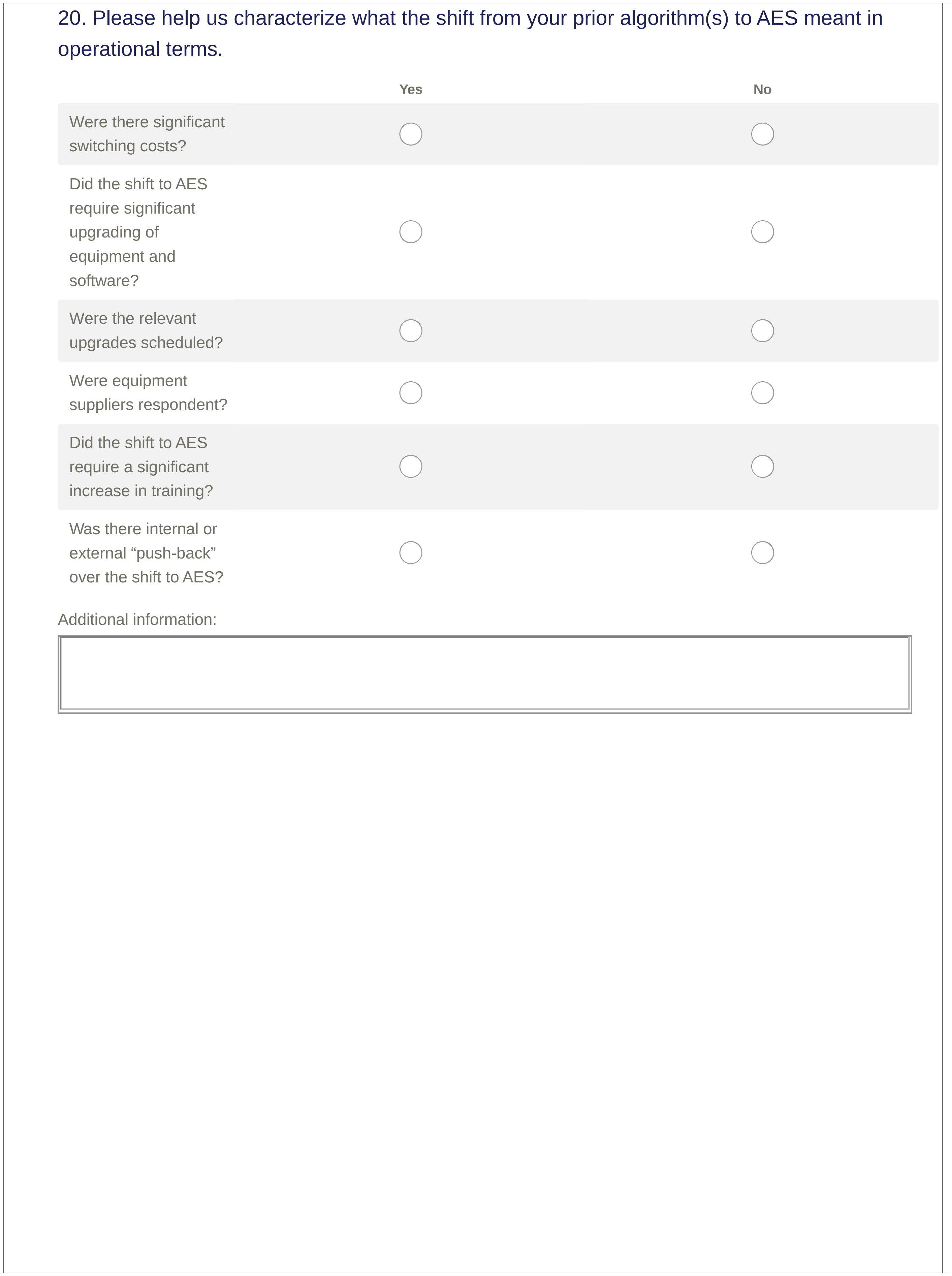
| | Year |
|---|---|
| First center/ provider adopted AES in: | |
| Last center/ provider adopted AES in: | |

Explanation (if needed)

19. What symmetric block encryption algorithm did the first and last AES adopters (data center, hosting service, cloud service) use immediately prior to AES adoption?

| | Algorithm Used Pre-AES |
|---|---|
| First adopter | |
| Last adopter | |

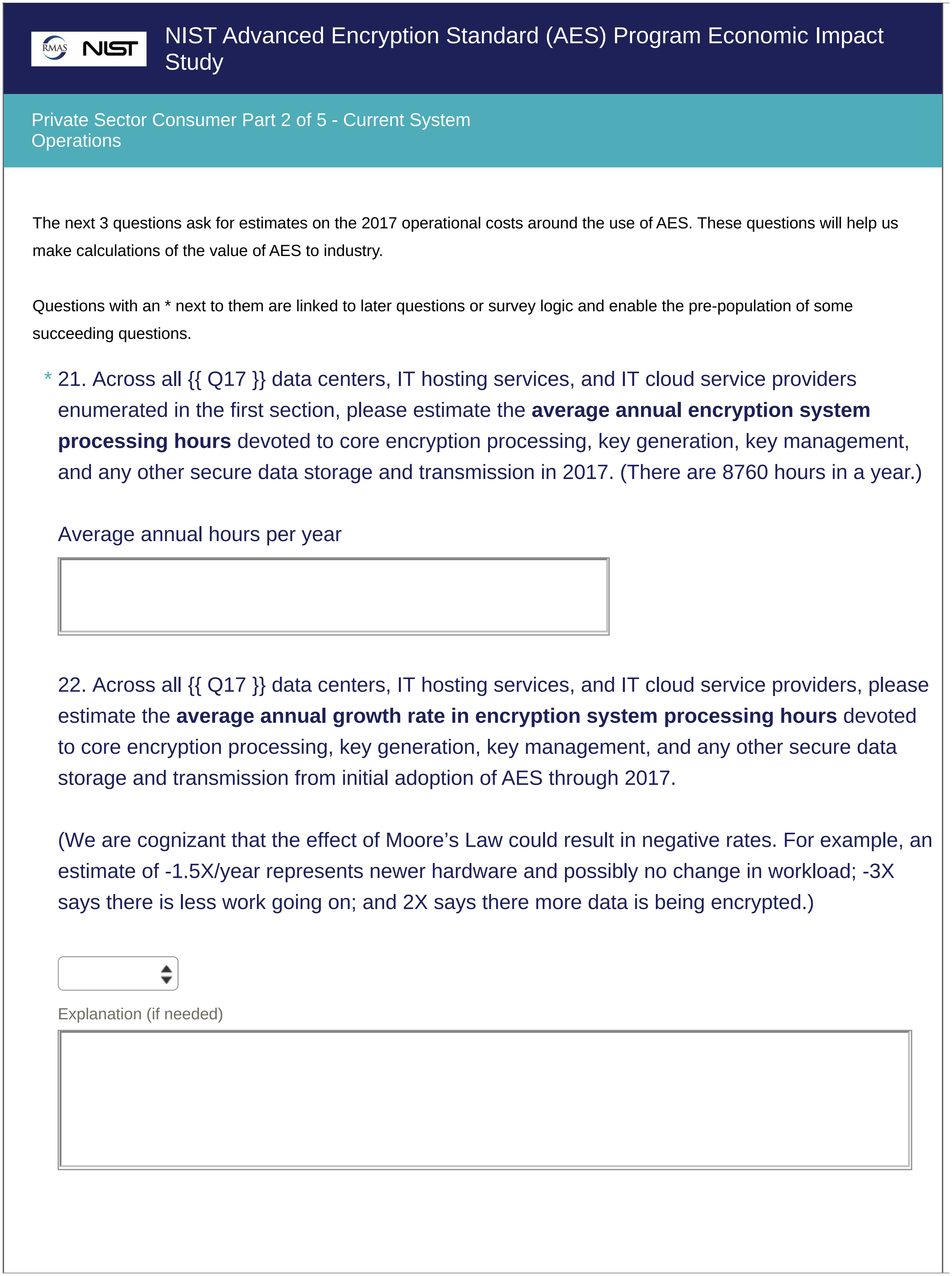
Explanation (if needed)



20. Please help us characterize what the shift from your prior algorithm(s) to AES meant in operational terms.

| | Yes | No |
|---|---|---|
| Were there significant switching costs? | ○ | ○ |
| Did the shift to AES require significant upgrading of equipment and software? | ○ | ○ |
| Were the relevant upgrades scheduled? | ○ | ○ |
| Were equipment suppliers respondent? | ○ | ○ |
| Did the shift to AES require a significant increase in training? | ○ | ○ |
| Was there internal or external “push-back” over the shift to AES? | ○ | ○ |

Additional information:



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Private Sector Consumer Part 2 of 5 - Current System Operations

The next 3 questions ask for estimates on the 2017 operational costs around the use of AES. These questions will help us make calculations of the value of AES to industry.

Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.

* 21. Across all {{ Q17 }} data centers, IT hosting services, and IT cloud service providers enumerated in the first section, please estimate the **average annual encryption system processing hours** devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission in 2017. (There are 8760 hours in a year.)

Average annual hours per year

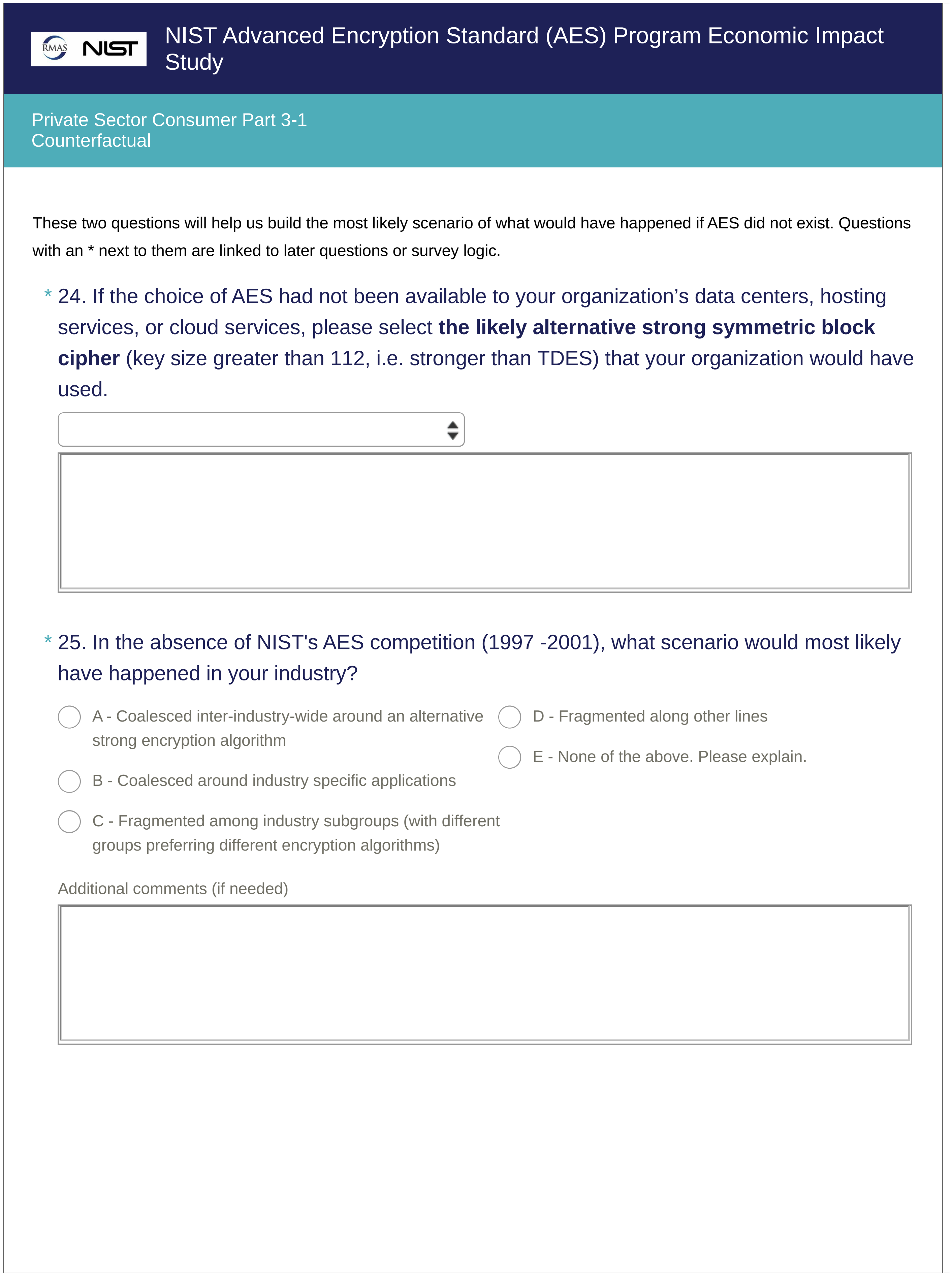
22. Across all {{ Q17 }} data centers, IT hosting services, and IT cloud service providers, please estimate the **average annual growth rate in encryption system processing hours** devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission from initial adoption of AES through 2017.

(We are cognizant that the effect of Moore’s Law could result in negative rates. For example, an estimate of -1.5X/year represents newer hardware and possibly no change in workload; -3X says there is less work going on; and 2X says there more data is being encrypted.)

Explanation (if needed)

* 23. For 2017, across all {{ Q17 }} data centers, IT hosting services, and IT cloud service providers, please estimate your **average encryption system budget** (US$) devoted to core encryption processing, key generation, key management, and any other secure data storage and transmission.

Average Encryption System Budget (US$)



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Private Sector Consumer Part 3-1
Counterfactual

These two questions will help us build the most likely scenario of what would have happened if AES did not exist. Questions with an * next to them are linked to later questions or survey logic.

* 24. If the choice of AES had not been available to your organization’s data centers, hosting services, or cloud services, please select **the likely alternative strong symmetric block cipher** (key size greater than 112, i.e. stronger than TDES) that your organization would have used.

* 25. In the absence of NIST's AES competition (1997 -2001), what scenario would most likely have happened in your industry?

○ A - Coalesced inter-industry-wide around an alternative strong encryption algorithm

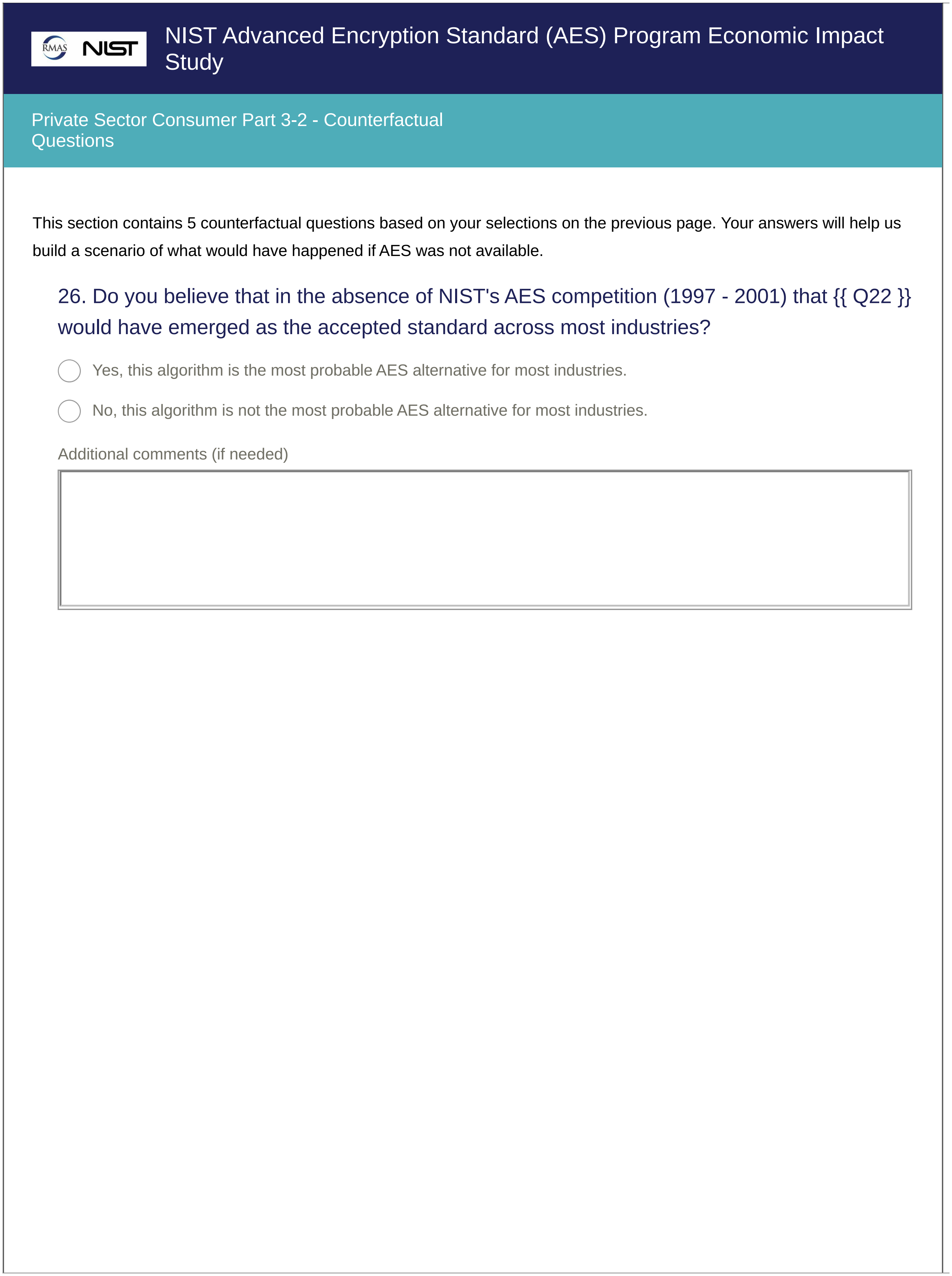
○ B - Coalesced around industry specific applications

○ C - Fragmented among industry subgroups (with different groups preferring different encryption algorithms)

○ D - Fragmented along other lines

○ E - None of the above. Please explain.

Additional comments (if needed)



RMAS NIST

NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Private Sector Consumer Part 3-2 - Counterfactual Questions

This section contains 5 counterfactual questions based on your selections on the previous page. Your answers will help us build a scenario of what would have happened if AES was not available.

26. Do you believe that in the absence of NIST's AES competition (1997 - 2001) that {{ Q22 }} would have emerged as the accepted standard across most industries?

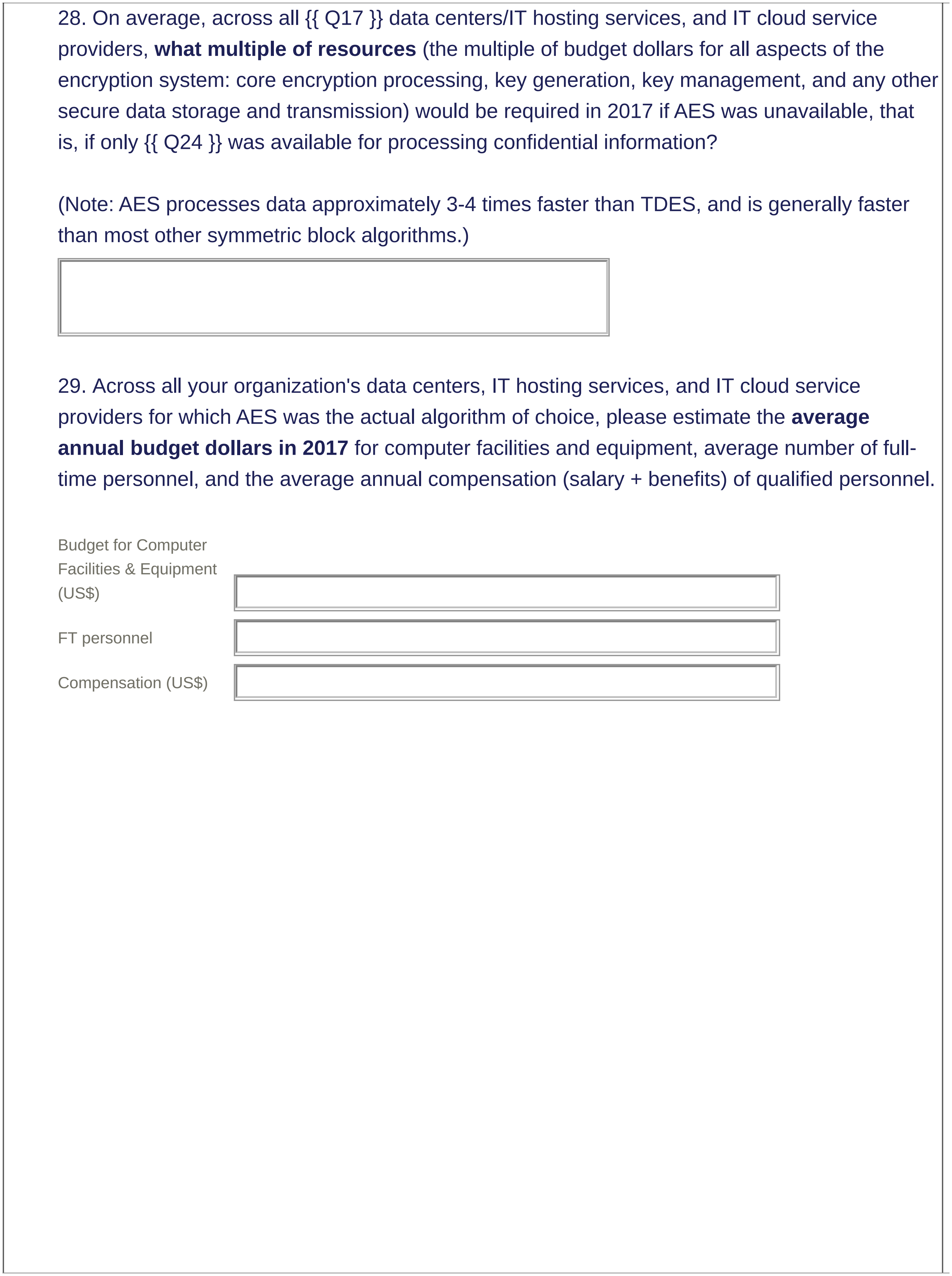
○ Yes, this algorithm is the most probable AES alternative for most industries.

○ No, this algorithm is not the most probable AES alternative for most industries.

Additional comments (if needed)

27. If you selected no, please provide the industries and the alternative algorithms you believe they would have coalesced around in the comments box below the table. Please use the 2-digit industry codes and algorithms in the table below to enter your answer as "industry code, algorithm".

| Industry | Algorithms |
|---|---|
| 11 - Agriculture, Forestry, Fishing and Hunting<br>21 - Mining<br>22 - Utilities<br>23 - Construction<br>31-33 - Manufacturing<br>42 - Wholesale Trade<br>44-45 - Retail Trade<br>48-49 - Transportation and Warehousing<br>51 - Information<br>52 - Finance and Insurance<br>53 - Real Estate Rental and Leasing<br>54 - Professional, Scientific, and Technical Services<br>55 - Management of Companies and Enterprises<br>56 - Administrative and Support and Waste Management and Remediation Services<br>61 - Educational Services<br>62 - Health Care and Social Assistance<br>71 - Arts, Entertainment, and Recreation<br>72 - Accommodation and Food Services<br>81 - Other Services (except Public Administration)<br>92 - Public Administration | Blowfish<br>Camellia<br>CAST-256<br>CRYPTON<br>DEAL<br>DFC<br>E2<br>FROG<br>HPC<br>IDEA<br>LOKI97<br>MAGENTA<br>MARS<br>Proprietary algorithms<br>RC5<br>RC6<br>SAFER+<br>SAFER K-128<br>Serpent<br>SQUARE<br>Twofish |



28. On average, across all {{ Q17 }} data centers/IT hosting services, and IT cloud service providers, **what multiple of resources** (the multiple of budget dollars for all aspects of the encryption system: core encryption processing, key generation, key management, and any other secure data storage and transmission) would be required in 2017 if AES was unavailable, that is, if only {{ Q24 }} was available for processing confidential information?

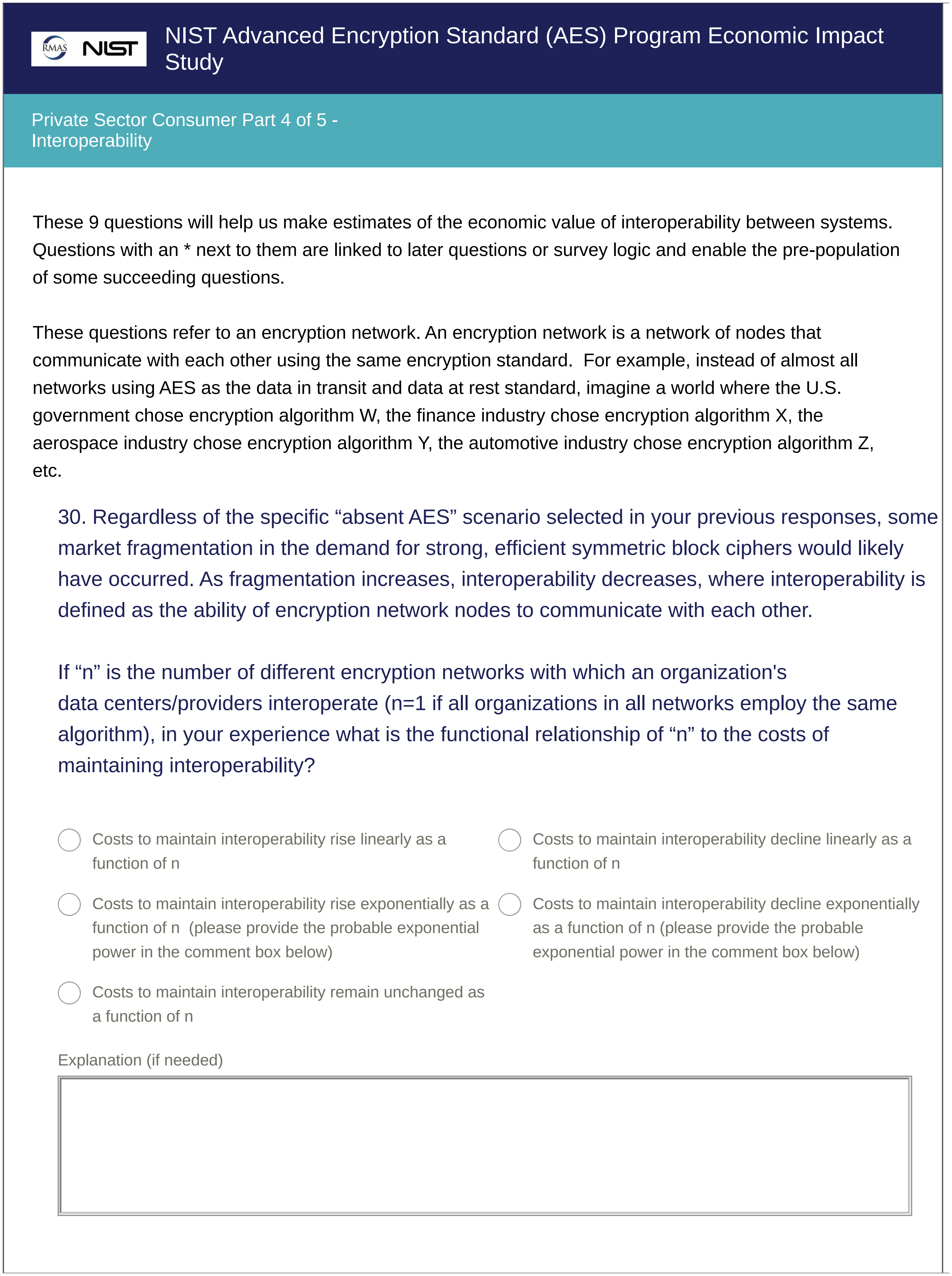
(Note: AES processes data approximately 3-4 times faster than TDES, and is generally faster than most other symmetric block algorithms.)

29. Across all your organization's data centers, IT hosting services, and IT cloud service providers for which AES was the actual algorithm of choice, please estimate the **average annual budget dollars in 2017** for computer facilities and equipment, average number of full-time personnel, and the average annual compensation (salary + benefits) of qualified personnel.

Budget for Computer Facilities & Equipment (US$)

FT personnel

Compensation (US$)



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Private Sector Consumer Part 4 of 5 -
Interoperability

These 9 questions will help us make estimates of the economic value of interoperability between systems. Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.

These questions refer to an encryption network. An encryption network is a network of nodes that communicate with each other using the same encryption standard.  For example, instead of almost all networks using AES as the data in transit and data at rest standard, imagine a world where the U.S. government chose encryption algorithm W, the finance industry chose encryption algorithm X, the aerospace industry chose encryption algorithm Y, the automotive industry chose encryption algorithm Z, etc.

30. Regardless of the specific “absent AES” scenario selected in your previous responses, some market fragmentation in the demand for strong, efficient symmetric block ciphers would likely have occurred. As fragmentation increases, interoperability decreases, where interoperability is defined as the ability of encryption network nodes to communicate with each other.

If “n” is the number of different encryption networks with which an organization's data centers/providers interoperate (n=1 if all organizations in all networks employ the same algorithm), in your experience what is the functional relationship of “n” to the costs of maintaining interoperability?

○ Costs to maintain interoperability rise linearly as a function of n

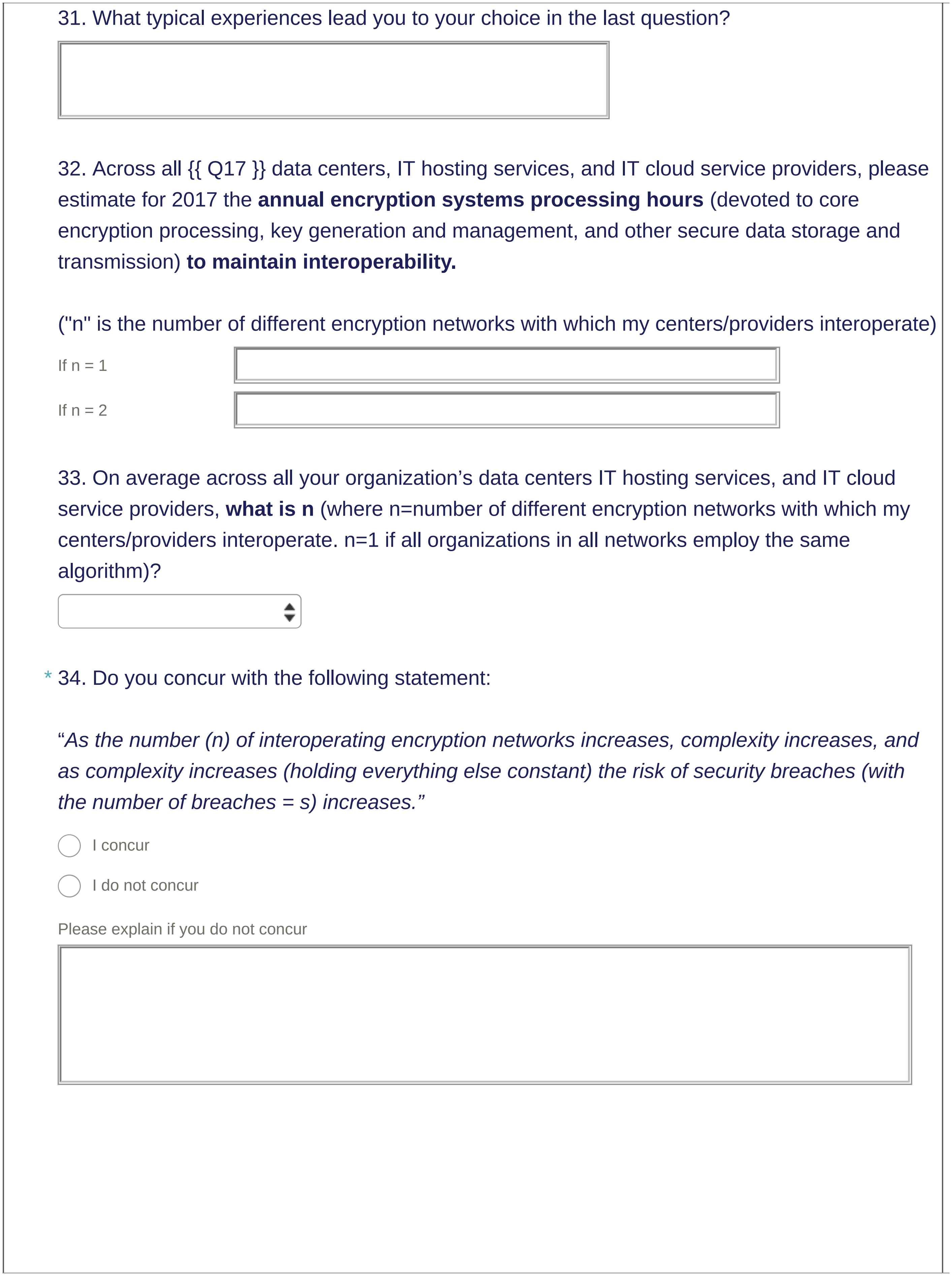
○ Costs to maintain interoperability decline linearly as a function of n

○ Costs to maintain interoperability rise exponentially as a function of n  (please provide the probable exponential power in the comment box below)

○ Costs to maintain interoperability decline exponentially as a function of n (please provide the probable exponential power in the comment box below)

○ Costs to maintain interoperability remain unchanged as a function of n

Explanation (if needed)



31. What typical experiences lead you to your choice in the last question?

32. Across all {{ Q17 }} data centers, IT hosting services, and IT cloud service providers, please estimate for 2017 the **annual encryption systems processing hours** (devoted to core encryption processing, key generation and management, and other secure data storage and transmission) **to maintain interoperability.**

("n" is the number of different encryption networks with which my centers/providers interoperate)

If n = 1

If n = 2

33. On average across all your organization’s data centers IT hosting services, and IT cloud service providers, **what is n** (where n=number of different encryption networks with which my centers/providers interoperate. n=1 if all organizations in all networks employ the same algorithm)?

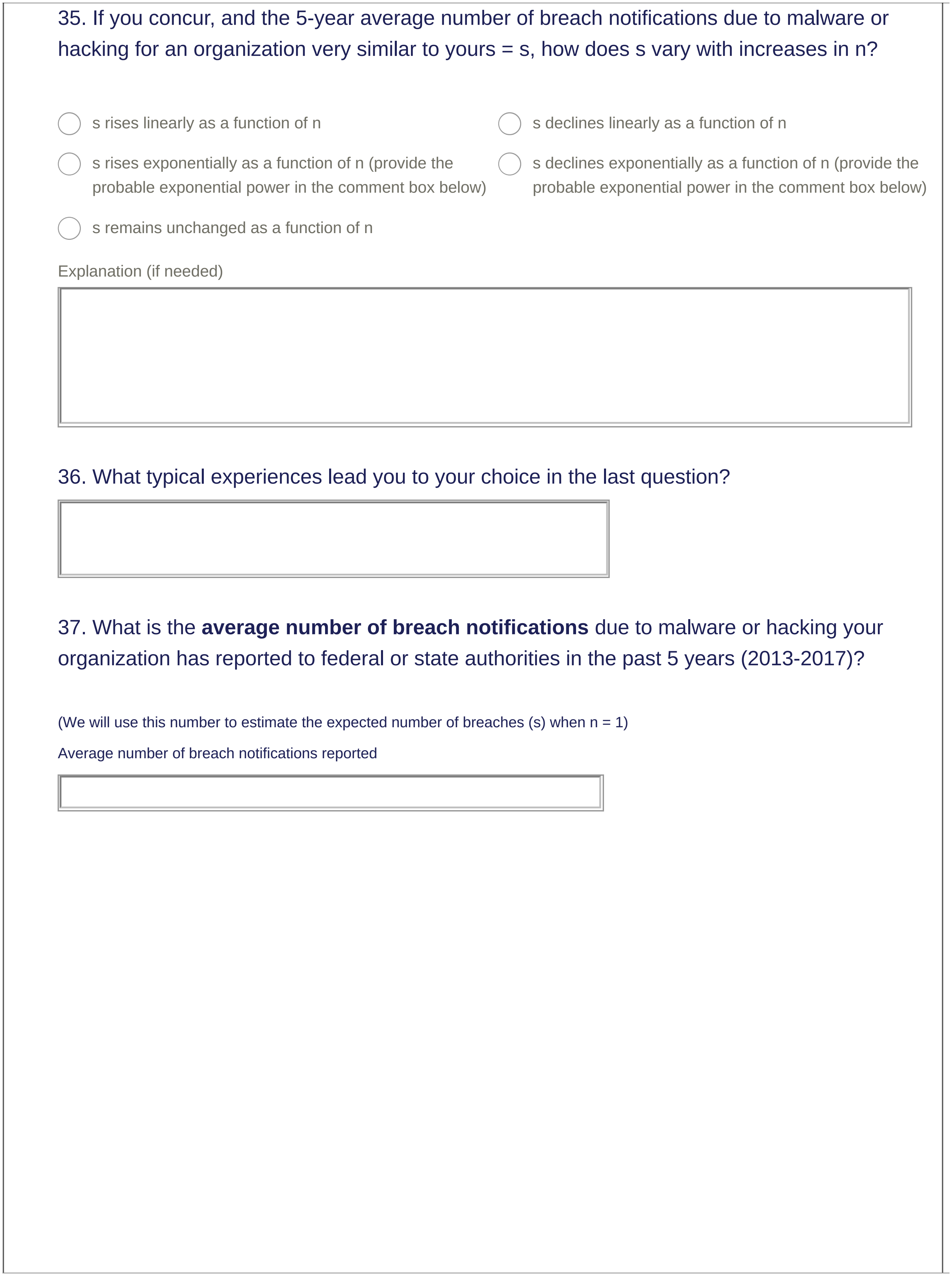
* 34. Do you concur with the following statement:

“*As the number (n) of interoperating encryption networks increases, complexity increases, and as complexity increases (holding everything else constant) the risk of security breaches (with the number of breaches = s) increases.”*

○ I concur

○ I do not concur

Please explain if you do not concur



35. If you concur, and the 5-year average number of breach notifications due to malware or hacking for an organization very similar to yours = s, how does s vary with increases in n?

○ s rises linearly as a function of n

○ s declines linearly as a function of n

○ s rises exponentially as a function of n (provide the probable exponential power in the comment box below)

○ s declines exponentially as a function of n (provide the probable exponential power in the comment box below)

○ s remains unchanged as a function of n

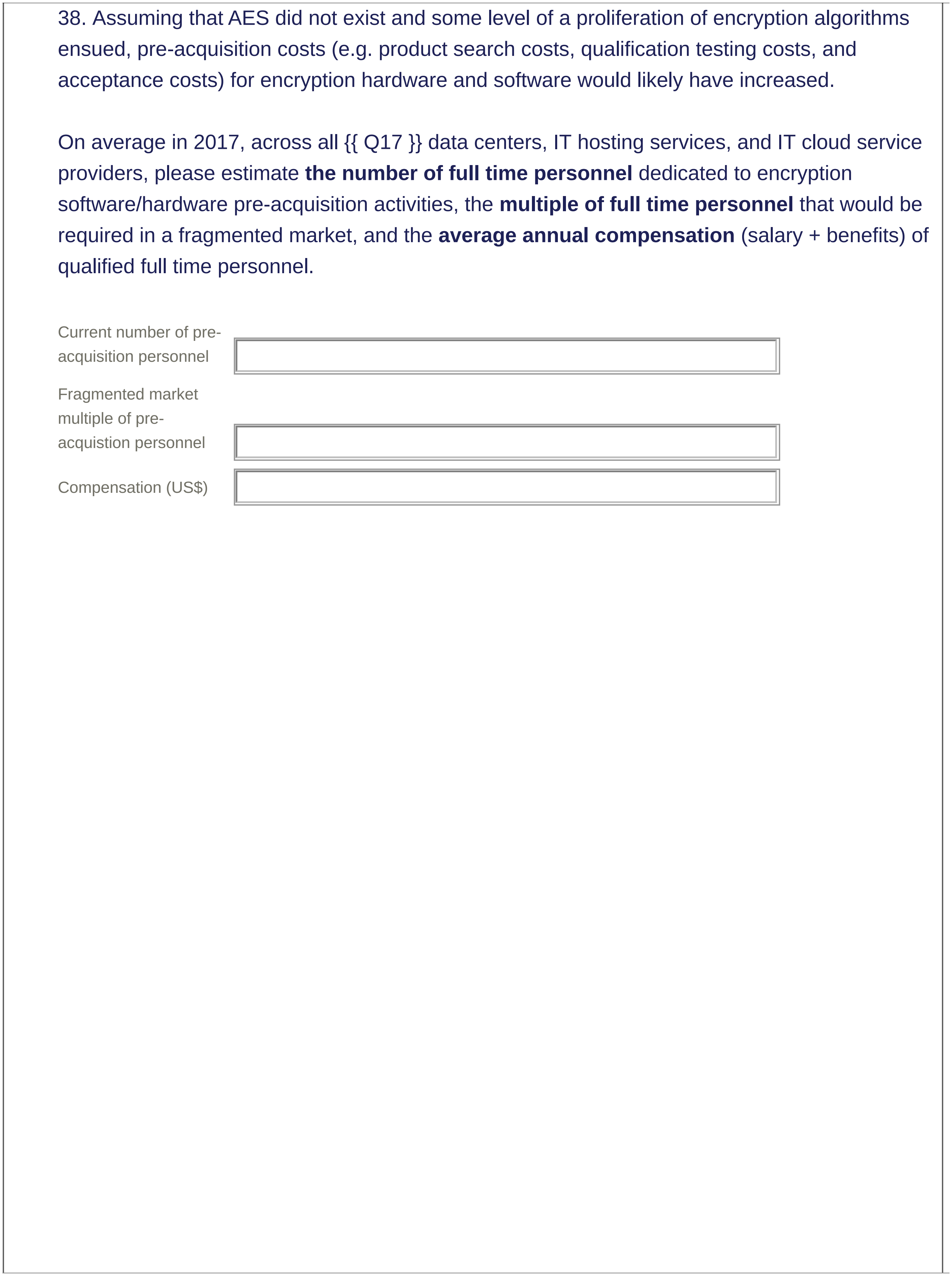
Explanation (if needed)

36. What typical experiences lead you to your choice in the last question?

37. What is the **average number of breach notifications** due to malware or hacking your organization has reported to federal or state authorities in the past 5 years (2013-2017)?

(We will use this number to estimate the expected number of breaches (s) when n = 1)

Average number of breach notifications reported



38. Assuming that AES did not exist and some level of a proliferation of encryption algorithms ensued, pre-acquisition costs (e.g. product search costs, qualification testing costs, and acceptance costs) for encryption hardware and software would likely have increased.

On average in 2017, across all {{ Q17 }} data centers, IT hosting services, and IT cloud service providers, please estimate **the number of full time personnel** dedicated to encryption software/hardware pre-acquisition activities, the **multiple of full time personnel** that would be required in a fragmented market, and the **average annual compensation** (salary + benefits) of qualified full time personnel.

Current number of pre-acquisition personnel

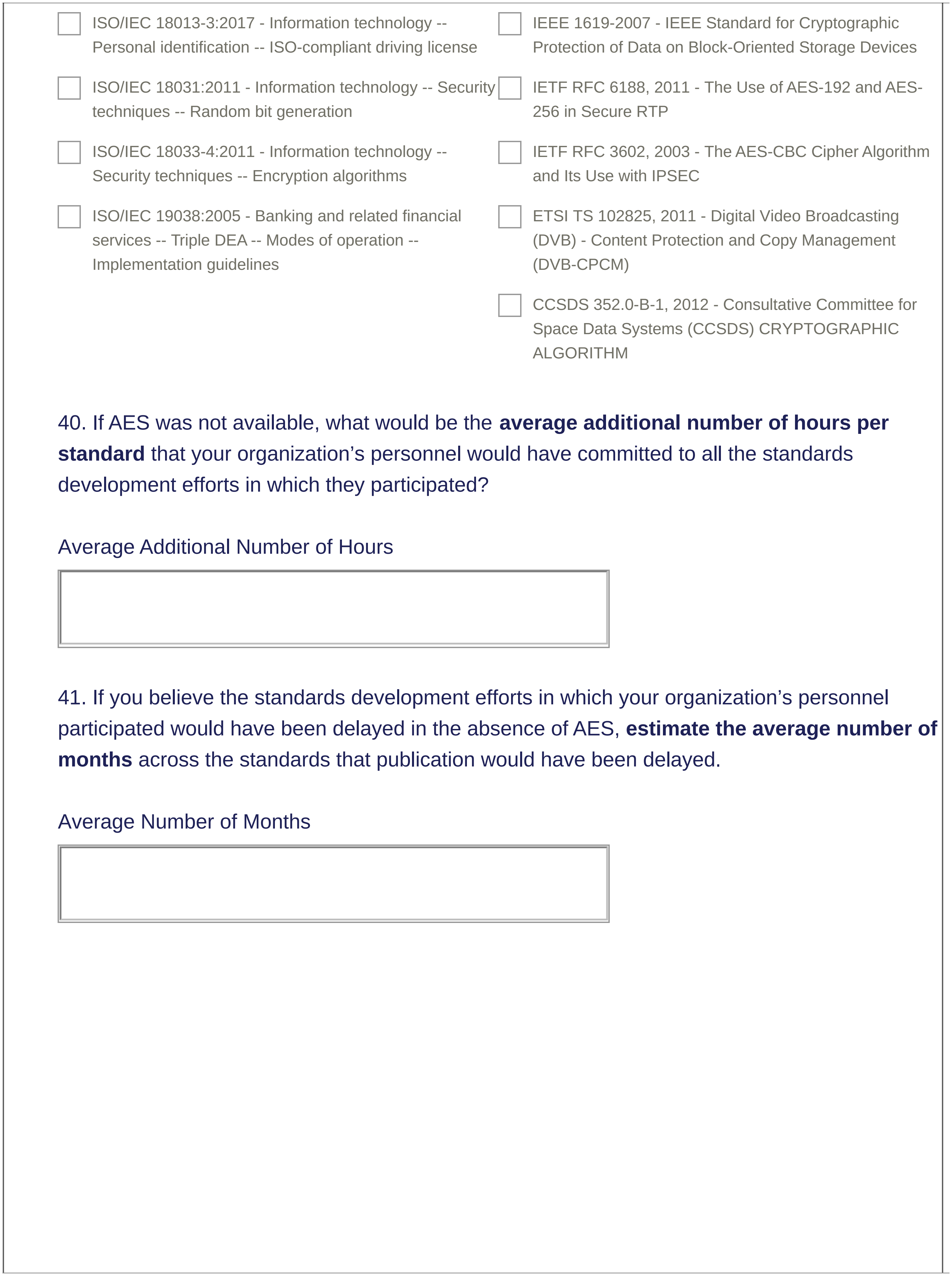
Fragmented market multiple of pre-acquistion personnel

Compensation (US$)

These last three questions refer to the diffusion of strong encryption technology as represented in the proliferation of international standards for which AES is regarded as “indispensible” (i.e. included as a normative reference).

39. Select all of the following consensus standards development efforts (and/or their U.S. counterparts) in which members of your organization participated.
This list includes standards from ISO, IEEE, IETF, and CCSDS.

- □ ISO/IEC 9564:2014 - Financial services — Personal Identification Number (PIN) management and security
- □ ISO/IEC 9797:2011 - Information technology -- Security techniques -- Message Authentication Codes (MACs)
- □ ISO/IEC 10116:2017 - Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
- □ ISO/IEC 11568:2012 - Financial services -- Key management (retail)
- □ ISO/IEC 11889:2015 - Information technology -- Trusted Platform Module
- □ ISO/IEC 13141:2015 - Electronic fee collection -- Localization augmentation communication for autonomous systems
- □ ISO/IEC 13157-2:2016 - Information technology -- Telecommunications and information exchange between systems -- NFC Security
- □ ISO/TR 13569:2005 - Financial services -- Information security guidelines
- □ ISO/IEC 14543:2010 - Information technology -- Home electronic system (HES) architecture
- □ ISO/IEC 15764:2004 - Road vehicles -- Extended data link security
- □ ISO/IEC 16504:2011 - Information technology -- Telecommunications and information exchange between systems -- MAC and PHY for operation in TV white space
- □ ISO/IEC 19772:2009 - Information technology -- Security techniques -- Authenticated encryption
- □ ISO/IEC 23001:2015 - Information technology -- MPEG systems technologies
- □ ISO/IEC DIS 23009:2013 - Information technology -- Dynamic adaptive streaming over HTTP (DASH)
- □ ISO/TS 24534:2011 - Road transport and Traffic Telematics - Automatic Vehicle and Equipment Identification - Electronic Registration Identification (ERI) for Vehicles
- □ ISO/IEC 24767:2009 - Information technology -- Home network security
- □ ISO/IEC 24771:2014 - Information technology -- Telecommunications and information exchange between systems -- MAC/PHY standard for ad hoc wireless network to support QoS in an industrial work environment
- □ ISO/IEC 25185:2016 - Identification cards -- Integrated circuit card authentication protocols
- □ ISO/IEC 26430:2008 - Digital cinema (D-cinema) operations
- □ IEEE 802.1 AE: 2006 - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
- □ IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages



□ ISO/IEC 18013-3:2017 - Information technology -- Personal identification -- ISO-compliant driving license

□ ISO/IEC 18031:2011 - Information technology -- Security techniques -- Random bit generation

□ ISO/IEC 18033-4:2011 - Information technology -- Security techniques -- Encryption algorithms

□ ISO/IEC 19038:2005 - Banking and related financial services -- Triple DEA -- Modes of operation -- Implementation guidelines

□ IEEE 1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

□ IETF RFC 6188, 2011 - The Use of AES-192 and AES-256 in Secure RTP

□ IETF RFC 3602, 2003 - The AES-CBC Cipher Algorithm and Its Use with IPSEC

□ ETSI TS 102825, 2011 - Digital Video Broadcasting (DVB) - Content Protection and Copy Management (DVB-CPCM)

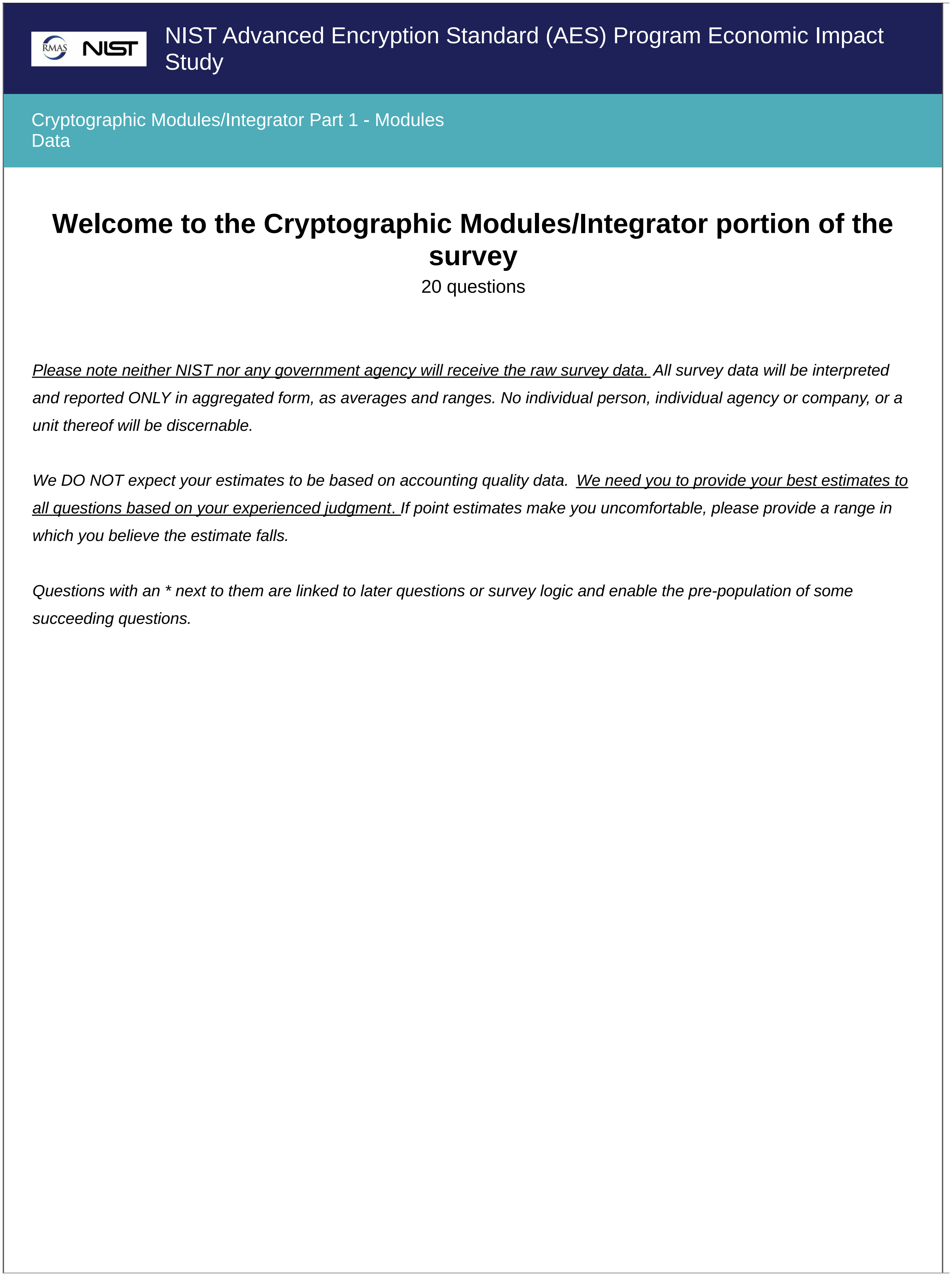
□ CCSDS 352.0-B-1, 2012 - Consultative Committee for Space Data Systems (CCSDS) CRYPTOGRAPHIC ALGORITHM

40. If AES was not available, what would be the **average additional number of hours per standard** that your organization’s personnel would have committed to all the standards development efforts in which they participated?

Average Additional Number of Hours

41. If you believe the standards development efforts in which your organization’s personnel participated would have been delayed in the absence of AES, **estimate the average number of months** across the standards that publication would have been delayed.

Average Number of Months



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Cryptographic Modules/Integrator Part 1 - Modules Data

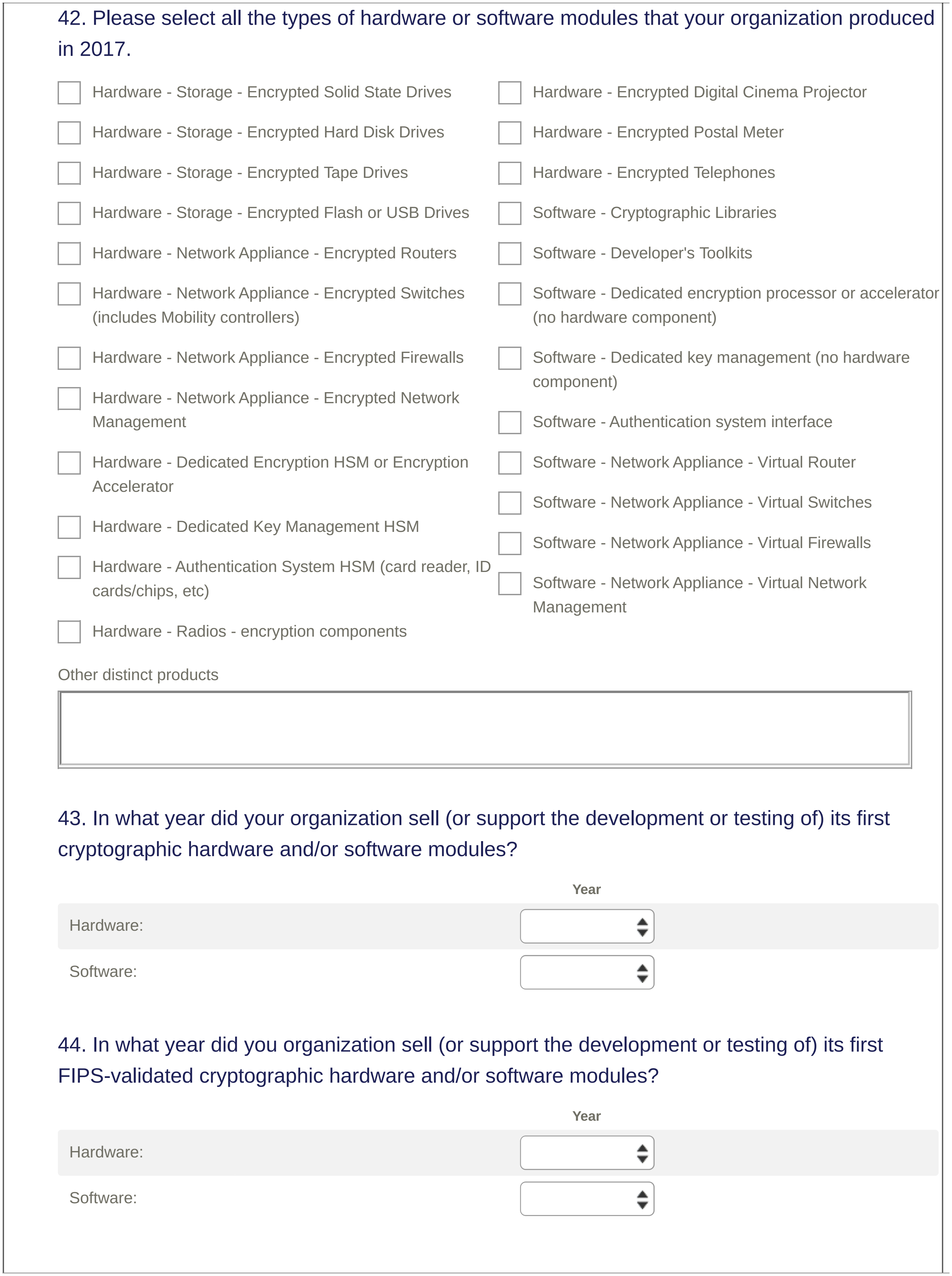
## Welcome to the Cryptographic Modules/Integrator portion of the survey

20 questions

*Please note neither NIST nor any government agency will receive the raw survey data. All survey data will be interpreted and reported ONLY in aggregated form, as averages and ranges. No individual person, individual agency or company, or a unit thereof will be discernable.*

*We DO NOT expect your estimates to be based on accounting quality data. We need you to provide your best estimates to all questions based on your experienced judgment. If point estimates make you uncomfortable, please provide a range in which you believe the estimate falls.*

*Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.*



42. Please select all the types of hardware or software modules that your organization produced in 2017.

□ Hardware - Storage - Encrypted Solid State Drives

□ Hardware - Storage - Encrypted Hard Disk Drives

□ Hardware - Storage - Encrypted Tape Drives

□ Hardware - Storage - Encrypted Flash or USB Drives

□ Hardware - Network Appliance - Encrypted Routers

□ Hardware - Network Appliance - Encrypted Switches (includes Mobility controllers)

□ Hardware - Network Appliance - Encrypted Firewalls

□ Hardware - Network Appliance - Encrypted Network Management

□ Hardware - Dedicated Encryption HSM or Encryption Accelerator

□ Hardware - Dedicated Key Management HSM

□ Hardware - Authentication System HSM (card reader, ID cards/chips, etc)

□ Hardware - Radios - encryption components

□ Hardware - Encrypted Digital Cinema Projector

□ Hardware - Encrypted Postal Meter

□ Hardware - Encrypted Telephones

□ Software - Cryptographic Libraries

□ Software - Developer's Toolkits

□ Software - Dedicated encryption processor or accelerator (no hardware component)

□ Software - Dedicated key management (no hardware component)

□ Software - Authentication system interface

□ Software - Network Appliance - Virtual Router

□ Software - Network Appliance - Virtual Switches

□ Software - Network Appliance - Virtual Firewalls

□ Software - Network Appliance - Virtual Network Management

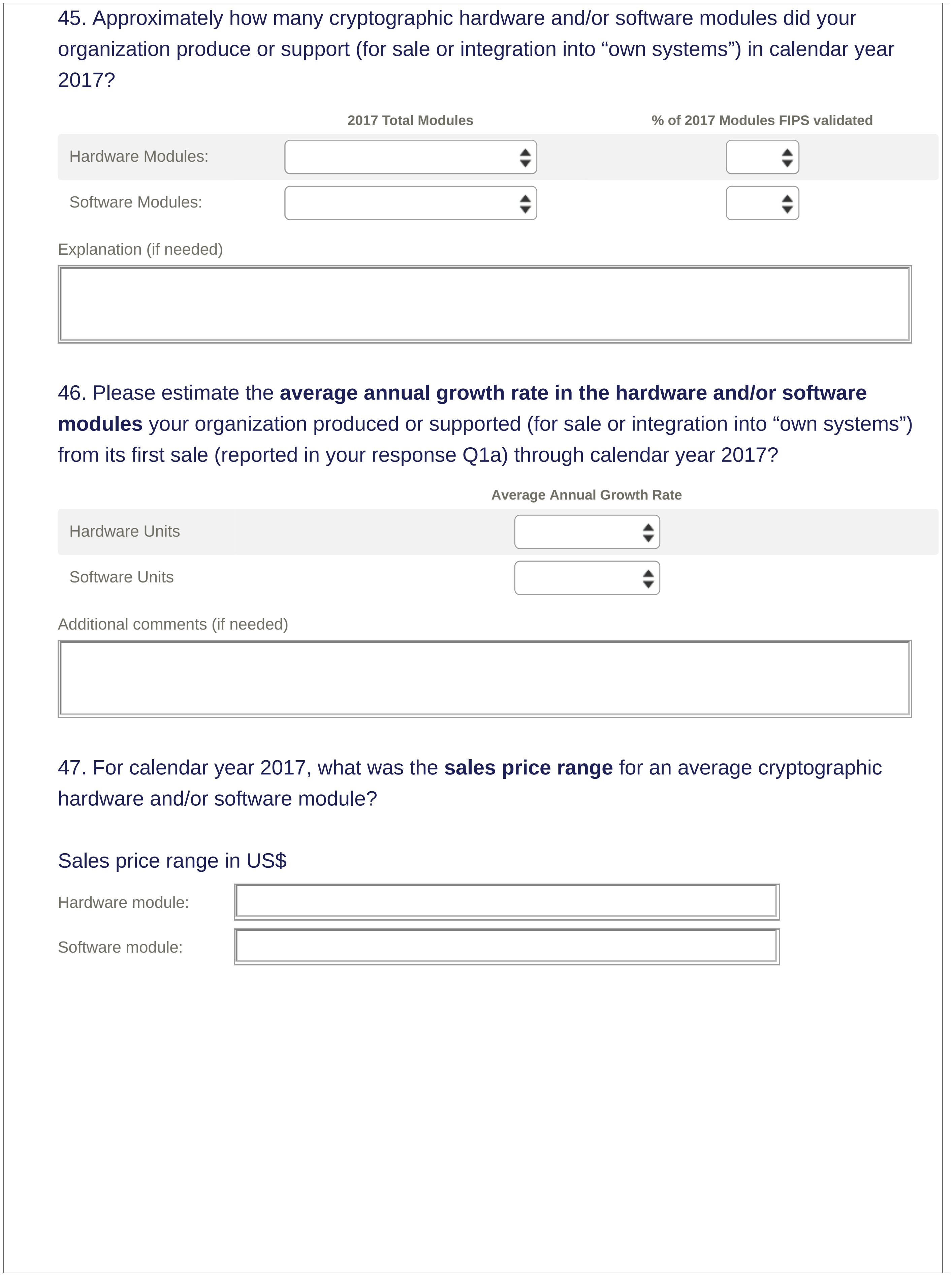
Other distinct products

43. In what year did your organization sell (or support the development or testing of) its first cryptographic hardware and/or software modules?

| | Year |
|---|---|
| Hardware: | |
| Software: | |

44. In what year did you organization sell (or support the development or testing of) its first FIPS-validated cryptographic hardware and/or software modules?

| | Year |
|---|---|
| Hardware: | |
| Software: | |



45. Approximately how many cryptographic hardware and/or software modules did your organization produce or support (for sale or integration into “own systems”) in calendar year 2017?

| | 2017 Total Modules | % of 2017 Modules FIPS validated |
|---|---|---|
| Hardware Modules: | | |
| Software Modules: | | |

Explanation (if needed)

46. Please estimate the **average annual growth rate in the hardware and/or software modules** your organization produced or supported (for sale or integration into “own systems”) from its first sale (reported in your response Q1a) through calendar year 2017?

| | Average Annual Growth Rate |
|---|---|
| Hardware Units | |
| Software Units | |

Additional comments (if needed)

47. For calendar year 2017, what was the **sales price range** for an average cryptographic hardware and/or software module?

Sales price range in US$

Hardware module:

Software module:

# NIST Advanced Encryption Standard (AES) Program Economic Impact Study

## Cryptographic Modules/Integrator Part 2 - Counterfactual Questions

Questions with an * next to them are linked to later questions or survey logic and enable the pre-population of some succeeding questions.

For the questions below, the following information may be useful:
We hypothesize that strong encryption (equal to or greater than 128 bits) was "in the wind" when NIST announced its intention to select a strong replacement for DES — through an open international competition — in 1997. Several strong symmetric block algorithms were already in existence, including the following:

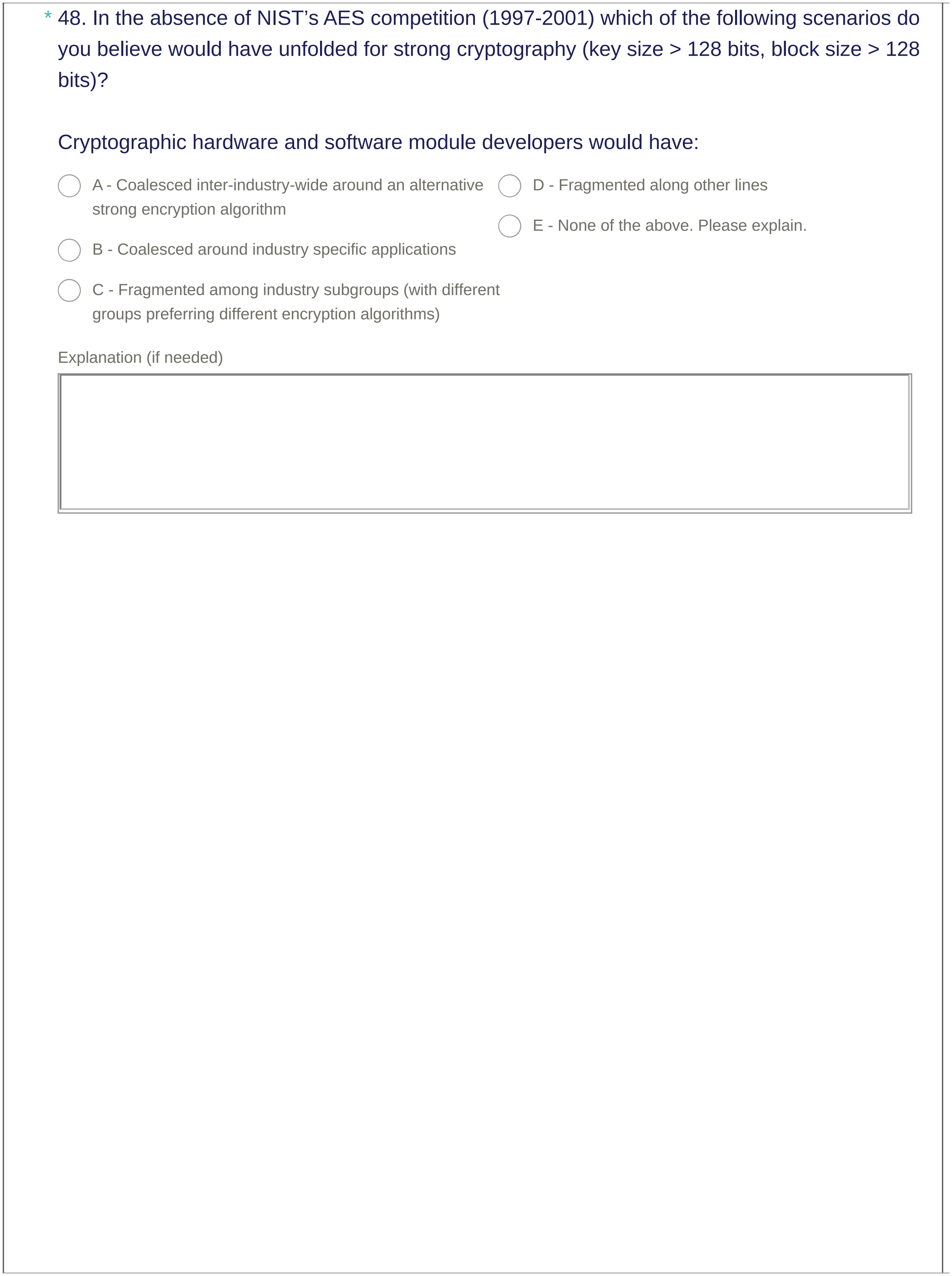
SQUARE (precursor to Rijndael), 1997, key size of 128 bits, and a block size of 128 bits

RC5 (precursor to RC6), 1994, key size up to 2048 bits, variety of block sizes

SAFER K-128 (precursor to SAFER+), key size of 128 bits, block size of 64 bits;

Blowfish (precursor to Twofish), 1991, key size of 32-448 bits, block size of 64 bits;

IDEA, 1991, key size of 128 bits, block size of 64 bits



* 48. In the absence of NIST’s AES competition (1997-2001) which of the following scenarios do you believe would have unfolded for strong cryptography (key size > 128 bits, block size > 128 bits)?

Cryptographic hardware and software module developers would have:

○ A - Coalesced inter-industry-wide around an alternative strong encryption algorithm

○ B - Coalesced around industry specific applications

○ C - Fragmented among industry subgroups (with different groups preferring different encryption algorithms)

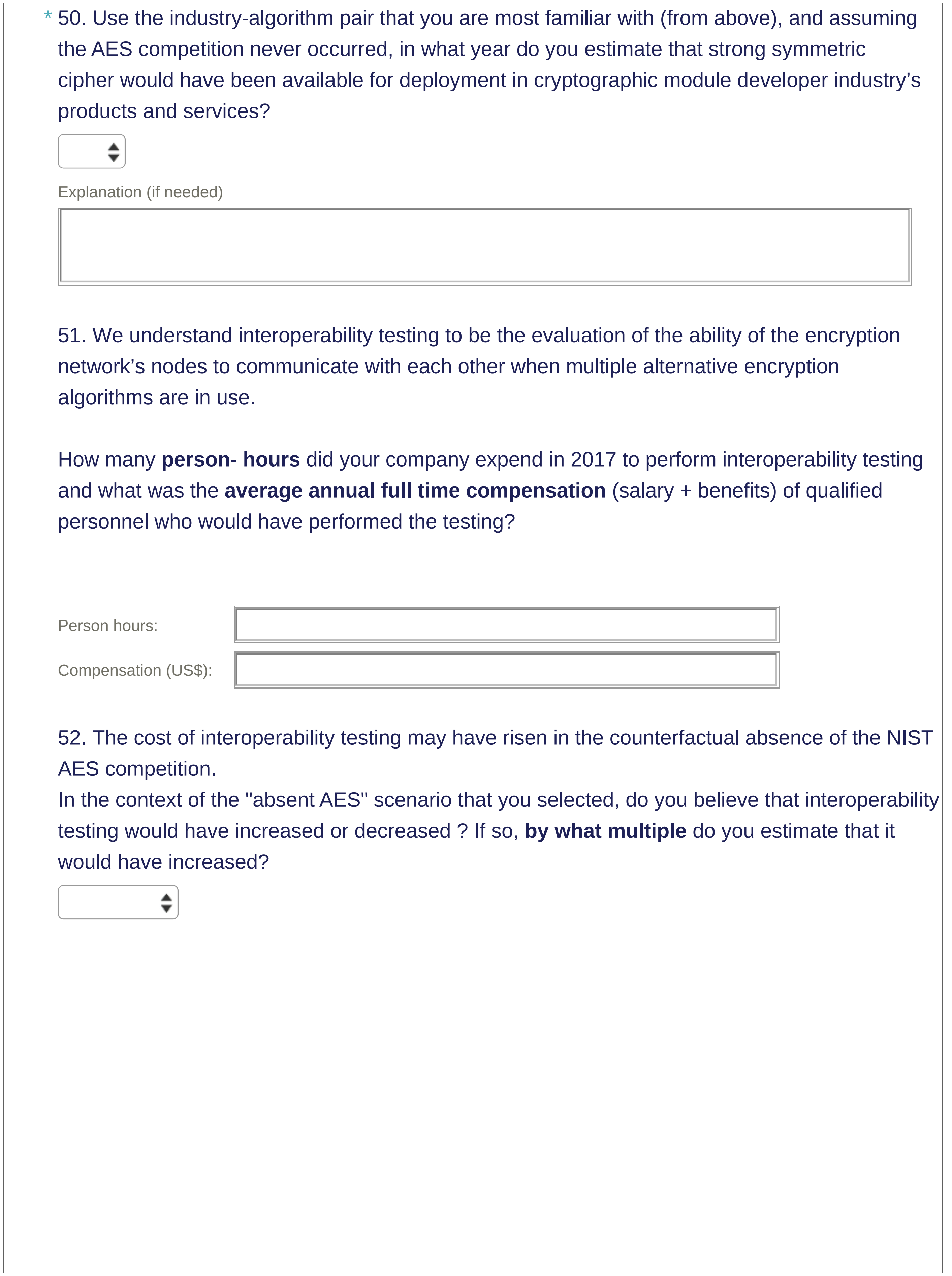
○ D - Fragmented along other lines

○ E - None of the above. Please explain.

Explanation (if needed)

49. Provide some examples of which industries would choose which algorithms in the scenario you selected above.
Please use the 2-digit industry codes and algorithms in the table below and format your answer as "industry code, algorithm."

| Industry | Algorithm |
|---|---|
| 11 - Agriculture, Forestry, Fishing and Hunting<br>21 - Mining<br>22 - Utilities<br>23 - Construction<br>31-33 - Manufacturing<br>42 - Wholesale Trade<br>44-45 - Retail Trade<br>48-49 - Transportation and Warehousing<br>51 - Information<br>52 - Finance and Insurance<br>53 - Real Estate Rental and Leasing<br>54 - Professional, Scientific, and Technical Services<br>55 - Management of Companies and Enterprises<br>56 - Administrative and Support and Waste Management and Remediation Services<br>61 - Educational Services<br>62 - Health Care and Social Assistance<br>71 - Arts, Entertainment, and Recreation<br>72 - Accommodation and Food Services<br>81 - Other Services (except Public Administration)<br>92 - Public Administration | Blowfish<br>Camellia<br>CAST-256<br>CRYPTON<br>DEAL<br>DFC<br>E2<br>FROG<br>HPC<br>IDEA<br>LOKI97<br>MAGENTA<br>MARS<br>Proprietary algorithms<br>RC5<br>RC6<br>SAFER+<br>SAFER K-128<br>Serpent<br>SQUARE<br>Twofish |



* 50. Use the industry-algorithm pair that you are most familiar with (from above), and assuming the AES competition never occurred, in what year do you estimate that strong symmetric cipher would have been available for deployment in cryptographic module developer industry’s products and services?

Explanation (if needed)

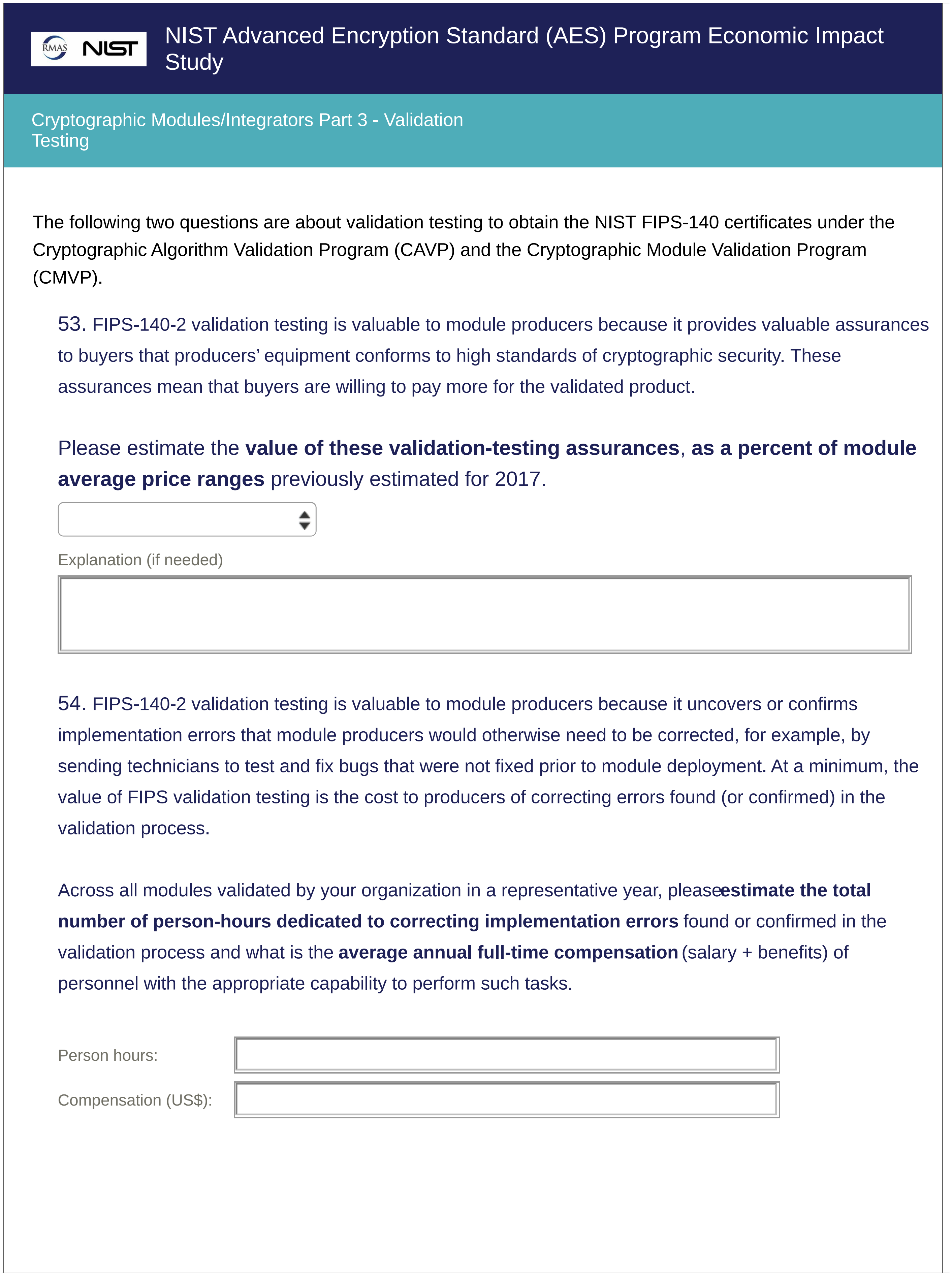
51. We understand interoperability testing to be the evaluation of the ability of the encryption network’s nodes to communicate with each other when multiple alternative encryption algorithms are in use.

How many **person- hours** did your company expend in 2017 to perform interoperability testing and what was the **average annual full time compensation** (salary + benefits) of qualified personnel who would have performed the testing?

Person hours:

Compensation (US$):

52. The cost of interoperability testing may have risen in the counterfactual absence of the NIST AES competition.
In the context of the "absent AES" scenario that you selected, do you believe that interoperability testing would have increased or decreased ? If so, **by what multiple** do you estimate that it would have increased?



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Cryptographic Modules/Integrators Part 3 - Validation Testing

The following two questions are about validation testing to obtain the NIST FIPS-140 certificates under the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP).

53. FIPS-140-2 validation testing is valuable to module producers because it provides valuable assurances to buyers that producers' equipment conforms to high standards of cryptographic security. These assurances mean that buyers are willing to pay more for the validated product.

Please estimate the **value of these validation-testing assurances**, **as a percent of module average price ranges** previously estimated for 2017.

Explanation (if needed)

54. FIPS-140-2 validation testing is valuable to module producers because it uncovers or confirms implementation errors that module producers would otherwise need to be corrected, for example, by sending technicians to test and fix bugs that were not fixed prior to module deployment. At a minimum, the value of FIPS validation testing is the cost to producers of correcting errors found (or confirmed) in the validation process.

Across all modules validated by your organization in a representative year, please**estimate the total number of person-hours dedicated to correcting implementation errors** found or confirmed in the validation process and what is the **average annual full-time compensation** (salary + benefits) of personnel with the appropriate capability to perform such tasks.

Person hours:

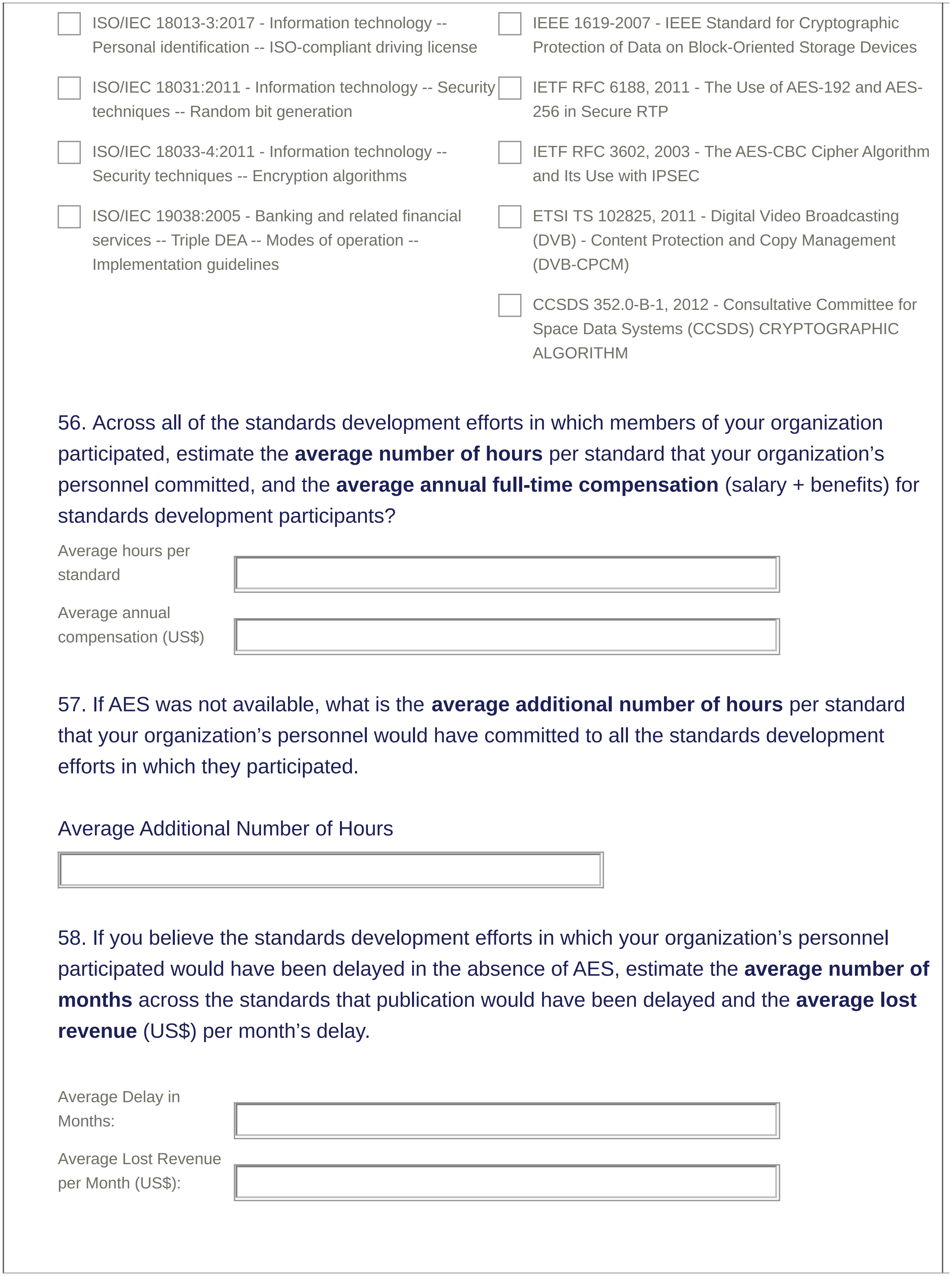
Compensation (US$):

## Cryptographic Modules/Integrator Part 4 - Standards Development

The following questions refer to the diffusion of strong encryption technology as represented in the proliferation of international standards for which AES is regarded as "indispensible" (i.e., included as a normative reference).

### 55. Select all of the following consensus standards development efforts (and/or their U.S. counterparts) in which members of your organization participated. This list includes standards from ISO, IEEE, IETF, and CCSDS.

- □ ISO/IEC 9564:2014 - Financial services — Personal Identification Number (PIN) management and security
- □ ISO/IEC 9797:2011 - Information technology -- Security techniques -- Message Authentication Codes (MACs)
- □ ISO/IEC 10116:2017 - Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
- □ ISO/IEC 11568:2012 - Financial services -- Key management (retail)
- □ ISO/IEC 11889:2015 - Information technology -- Trusted Platform Module
- □ ISO/IEC 13141:2015 - Electronic fee collection -- Localization augmentation communication for autonomous systems
- □ ISO/IEC 13157-2:2016 - Information technology -- Telecommunications and information exchange between systems -- NFC Security
- □ ISO/TR 13569:2005 - Financial services -- Information security guidelines
- □ ISO/IEC 14543:2010 - Information technology -- Home electronic system (HES) architecture
- □ ISO/IEC 15764:2004 - Road vehicles -- Extended data link security
- □ ISO/IEC 16504:2011 - Information technology -- Telecommunications and information exchange between systems -- MAC and PHY for operation in TV white space
- □ ISO/IEC 19772:2009 - Information technology -- Security techniques -- Authenticated encryption
- □ ISO/IEC 23001:2015 - Information technology -- MPEG systems technologies
- □ ISO/IEC DIS 23009:2013 - Information technology -- Dynamic adaptive streaming over HTTP (DASH)
- □ ISO/TS 24534:2011 - Road transport and Traffic Telematics - Automatic Vehicle and Equipment Identification - Electronic Registration Identification (ERI) for Vehicles
- □ ISO/IEC 24767:2009 - Information technology -- Home network security
- □ ISO/IEC 24771:2014 - Information technology -- Telecommunications and information exchange between systems -- MAC/PHY standard for ad hoc wireless network to support QoS in an industrial work environment
- □ ISO/IEC 25185:2016 - Identification cards -- Integrated circuit card authentication protocols
- □ ISO/IEC 26430:2008 - Digital cinema (D-cinema) operations
- □ IEEE 802.1 AE: 2006 - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
- □ IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages



□ ISO/IEC 18013-3:2017 - Information technology -- Personal identification -- ISO-compliant driving license

□ ISO/IEC 18031:2011 - Information technology -- Security techniques -- Random bit generation

□ ISO/IEC 18033-4:2011 - Information technology -- Security techniques -- Encryption algorithms

□ ISO/IEC 19038:2005 - Banking and related financial services -- Triple DEA -- Modes of operation -- Implementation guidelines

□ IEEE 1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

□ IETF RFC 6188, 2011 - The Use of AES-192 and AES-256 in Secure RTP

□ IETF RFC 3602, 2003 - The AES-CBC Cipher Algorithm and Its Use with IPSEC

□ ETSI TS 102825, 2011 - Digital Video Broadcasting (DVB) - Content Protection and Copy Management (DVB-CPCM)

□ CCSDS 352.0-B-1, 2012 - Consultative Committee for Space Data Systems (CCSDS) CRYPTOGRAPHIC ALGORITHM

56. Across all of the standards development efforts in which members of your organization participated, estimate the **average number of hours** per standard that your organization's personnel committed, and the **average annual full-time compensation** (salary + benefits) for standards development participants?

Average hours per standard

Average annual compensation (US$)

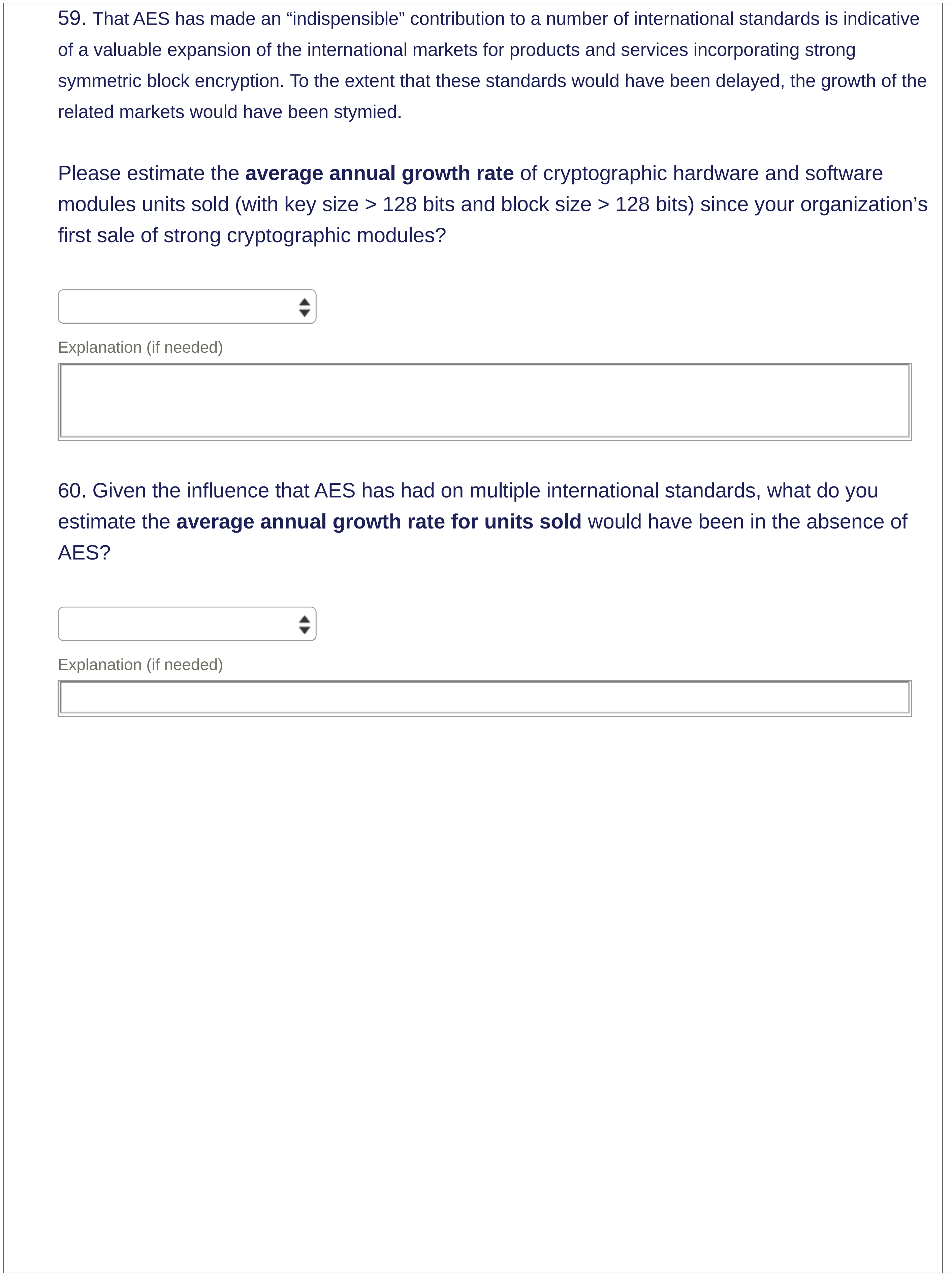
57. If AES was not available, what is the **average additional number of hours** per standard that your organization's personnel would have committed to all the standards development efforts in which they participated.

Average Additional Number of Hours

58. If you believe the standards development efforts in which your organization's personnel participated would have been delayed in the absence of AES, estimate the **average number of months** across the standards that publication would have been delayed and the **average lost revenue** (US$) per month's delay.

Average Delay in Months:

Average Lost Revenue per Month (US$):



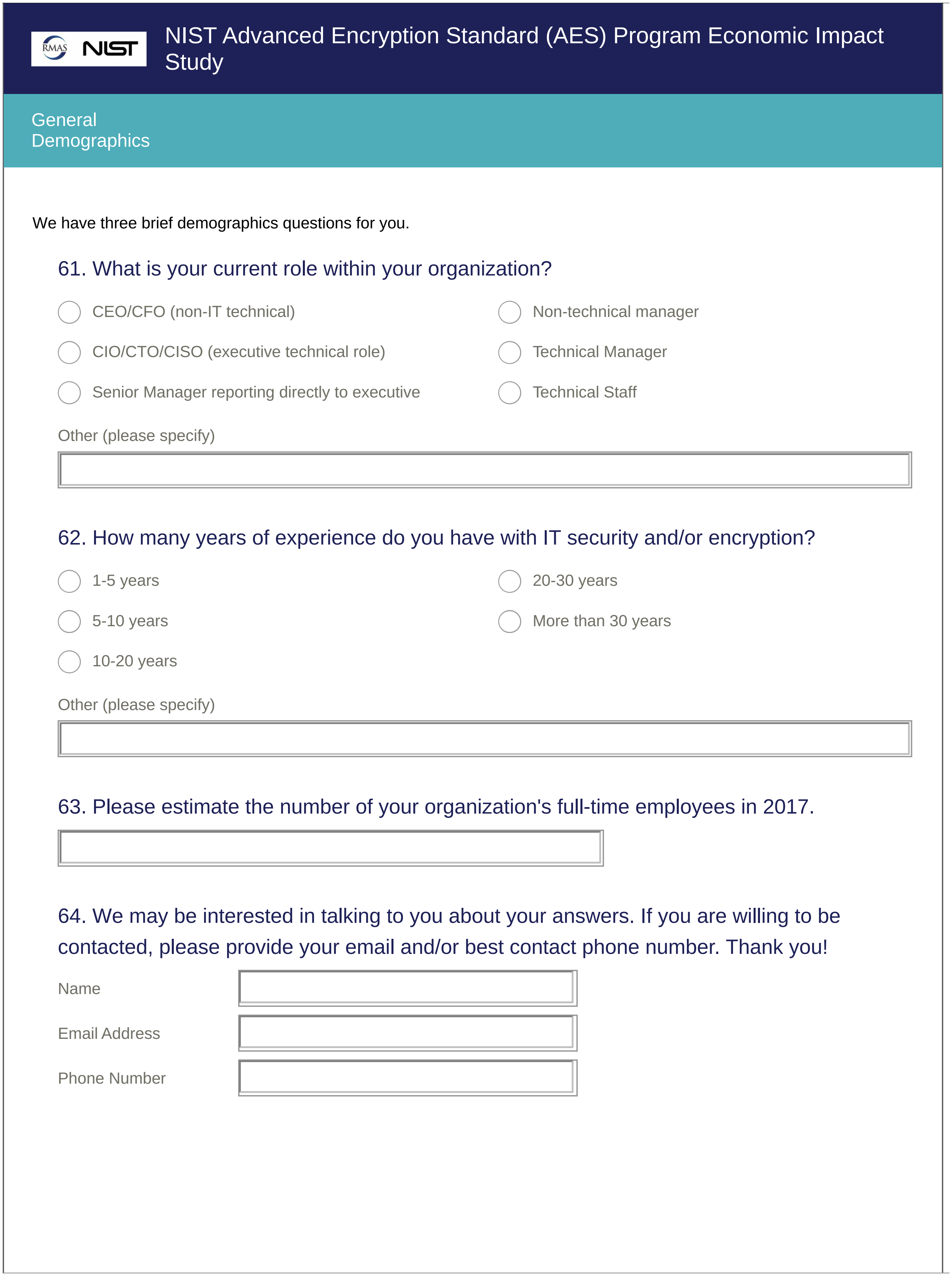
59. That AES has made an “indispensible” contribution to a number of international standards is indicative of a valuable expansion of the international markets for products and services incorporating strong symmetric block encryption. To the extent that these standards would have been delayed, the growth of the related markets would have been stymied.

Please estimate the **average annual growth rate** of cryptographic hardware and software modules units sold (with key size > 128 bits and block size > 128 bits) since your organization’s first sale of strong cryptographic modules?

Explanation (if needed)

60. Given the influence that AES has had on multiple international standards, what do you estimate the **average annual growth rate for units sold** would have been in the absence of AES?

Explanation (if needed)



NIST Advanced Encryption Standard (AES) Program Economic Impact Study

General Demographics

We have three brief demographics questions for you.

61. What is your current role within your organization?

○ CEO/CFO (non-IT technical)

○ CIO/CTO/CISO (executive technical role)

○ Senior Manager reporting directly to executive

○ Non-technical manager

○ Technical Manager

○ Technical Staff

Other (please specify)

62. How many years of experience do you have with IT security and/or encryption?

○ 1-5 years

○ 5-10 years

○ 10-20 years

○ 20-30 years

○ More than 30 years

Other (please specify)

63. Please estimate the number of your organization's full-time employees in 2017.

64. We may be interested in talking to you about your answers. If you are willing to be contacted, please provide your email and/or best contact phone number. Thank you!

Name

Email Address

Phone Number

# Appendix C. Economic Impact Metrics

The economic impact metrics in this report are calculated from a time series of costs and benefits in constant dollars. They represent "real" rates of return. In contrast, "nominal" rates of return would be based on time series of current dollars (the dollars of the year in which the benefits were realized or in which the costs were incurred).

## Internal Rate of Return (IRR)

The IRR is the value of the discount rate, i, that equates the net present value (NPV) of a stream of all net benefits associated with an investment project to zero. The time series runs from the beginning of the project, t = 0, to a milestone terminal point, t = n. Net benefits refer to total benefits (B) less total costs (C) in each time period. Mathematically,

$$(1)\ NPV = [(B_0 - C_0) / (1 + i)^0] + \ldots + [(B_n - C_n) / (1 + i)^n] = 0$$

where $(B_t - C_t)$ represents the net benefits associated with the project in year t, and n represents the number of time periods (years in most cases) being considered in the evaluation.

For unique solutions of i, from equation (1), the IRR can be compared to a value, r, that represents the opportunity cost of funds invested by the technology-based public institution. Thus, if the opportunity cost of funds is less than the social rate of return, the project was worthwhile from an ex post social perspective.

## Benefit-to-Cost Ratio (B/C)

The ratio of benefits-to-costs is precisely that, the ratio of the present value of all measured benefits to the present value of all costs. Both benefits and costs are referenced to the initial time period, t = 0, as:

$$(2)\ B / C = [\Sigma_{t=0 \text{ to } t=n} B_t /(1 + r)^t] / [\Sigma_{t=0 \text{ to } t=n} C_t / (1 + r)^t]$$

A benefit-to-cost ratio of 1 implies a break-even project. Any project with B / C > 1 is a relatively successful project. Fundamental to implementing the ratio of benefits-to-costs is a value for the discount rate, r.

While the discount rate representing the opportunity cost for public funds could differ across a portfolio of public investments, the calculated metrics in this report follow the guidelines set forth by the Office of Management and Budget: Constant-dollar benefit-cost analyses of proposed investments and regulations should report net present value and other outcomes determined using a real discount rate of 7%.[150]

### Net Present Value (NPV)

The information developed to determine the benefit-to-cost ratio can be used to determine net present value as:

$$(3)\ \text{NPV} = \text{B} - \text{C}.$$

[150] Office of Management and Budget (OMB), Circular No. A-94 Revised, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs," October 29, 1992.

## Appendix D. Understanding the Alternative IRR

The alternative IRR is a constrained and dampened IRR. As compared with the traditional internal rate of return, the alternative rate of return is much lower because it constrains all of the benefits to be reinvested, at the time they are realized, at the relatively low social required rate of return, and then the alternative internal rate of return is for the rate of growth in the returns over the entire period from 1996 to 2017, with the growth constrained to the lower 7% rate of return from the realization of the benefits until 2017.

Rather than "take down" the benefits in the year received, annual benefits must be invested at the social rate of return and allowed to grow until 2017. The benefits are cumulated in that way and then they are "taken down" in 2017. Thus, with a project such as the AES project, an initial investment pays a very large return in a few years. The traditional internal rate of return reflects that high rate of return when relatively few dollars invested initially yield a great many dollars in a few years. However, with the alternative internal rate of return, those great many dollars are not taken down or withdrawn at the time of the benefit and the high rate of return then observed. Instead, they are reinvested at the relatively low social required rate of return (the long-term average private rate of return on investment in the U.S. economy).[151] Then, years later in 2017, the return is taken down, i.e., withdrawn, and after years of growing at the lower rate of return the overall annual rate of return is dampened from what it would have been if the return had been withdrawn when it originally occurred and the internal rate of return recorded at that time.

The alternative internal rate of return is the rate at which the discounted present value of costs at time zero—the beginning of the investments in 1996—would have had to grow to release the cumulated value of the annual benefits that are taken down in 2017. In contrast, the traditional metric assumes that the benefits are growing at a certain rate—that they can be reinvested at that rate throughout the investment period until 2017—

[151] Link and Scott, 2011, op. cit.

making the entire stream of benefits with its returns dispersed over the years from the initiation of the project until 2017, have a present value in 1996 equal to the present value of the stream of costs at that time.  In the alternative, the annual benefits must be reinvested at the 7% annual rate of return and allowed to cumulate until 2017.  Then, at that time, with the growth rate in returns dampened to the 7% annual return from their actual occurrence until 2017, we find the rate that would make the cumulated 2017 amount's present value in 1996 equal to the present value of the stream of costs in 1996.

Here is a simple example.  Imagine for $100 invested now, there is a benefit of $150 in one year and then a benefit of $225 in two years.  The conventional internal rate of return is r such that 100 = 150/(1+r) + 225/(1+r)^2.  Then r = 1.42705 or 142.7%.  The alternative internal rate of return is r such that 100 = ((150)*(1.07) + 225)/(1+r)^2.  Then r = 0.963415 or 96.3%.  Even in this simple example, there is a dramatic dampening effect by not taking down the benefit of $150 in a year and reckoning the rate of return, but instead reinvesting it at the lower 7% per annum rate of return and then finding the rate of return over the longer period during which the return was constrained to the low 7% per annum.

# Appendix E. Two-Stage Procedure for Extrapolating the Economic Benefits of NIST's AES program

## Methodological Rationale for Benefits Extrapolation

The benefit estimates for the 169 survey respondents are understood as random variables subject to a great deal of uncertainty. The most important part of that uncertainty cannot be quantified because it is the uncertainty associated with the original set of 74 respondents that provided sufficient information to estimate AES benefits. Each of those 74 respondents typically did not provide enough information to quantify all of the types of benefits addressed in the survey. Although they often acknowledged that the benefits existed, they did not attempt to answers the survey questions that would have allowed a quantitative estimate. Even when sufficient information was provided to form an estimate of a particular type of benefit, the respondents were providing their knowledgeable assessment of the information, and those assessments are subject to uncertainty.

For the additional 95 respondents that provided the information used in the estimated model of benefits, the 95 predicted values for the present value of benefits in 2017 which are random variables, and there are two sources of their variance. One source of variance in the predicted values is the uncertainty associated with the estimated coefficients in our estimated model. The other source of variance is the residual error, the error in the estimated equation of our ordinary least squares model. Thus, the total for the estimated benefits for the two groups of respondents—the 74 respondents (for which we had their reported benefits) and the 95 respondents (who did not provide information about their benefits but did provide the information needed for the variables in our estimated model) is a random variable. It will have variance due to the incompleteness and uncertainty in the survey responses from the original 74 respondents, and then additionally from the two sources of variance in the 95 estimated benefits using our model.

The economic impact metrics reported in the body of the report should be considered to underestimate the AES benefit in the sense that typically respondents recognized, but could not quantify, many of the benefits asked about in the survey. Also, the impact metrics are subject to great uncertainty. They are the expected value of a portion of the benefits, and the probability distribution for that portion of the benefits assigns probability to much lower as well as much higher ranges for the benefits, although we cannot sensibly quantify the uncertainty because the most important part of it comes from the uncertainty surrounding the survey responses of the original 74 respondents rather than from the estimation of a formal model.

### First-Stage Extrapolation Procedure for 169 Survey Respondents

To estimate the benefits for the 95 survey respondents that did not provide information from which cost avoidance benefits could be directly estimated, the first step was to take the time series of annual benefits (in 2017 constant dollars) for each of our 74 respondents that provided data from which benefits estimates could be derived directly, and convert it to the present value of those benefits in 2017 (referred to in the body of the report as "cumulative benefits"). That present value of benefits in 2017 for each of the 74 observations is the value that would be generated by 2017 if each respondent's annual benefits, in its stream of benefits from 1998 to 2017, were invested at the real social annual rate of return of 7% and allowed to grow until 2017.[152]

The second step was to use those 74 respondents' cumulative benefits and industry sectors and respondent types to estimate a model of the 2017 present value of benefits. The model is an ordinary least squares regression of the 2017 present value of respondents' benefits as a function of the type of respondent (private consumer, private producer/developer, private integrator, public consumer, academic or independent cryptographer, and cryptographic testing consultants), and the industrial classification category(ies) for the respondent. The estimated model is significant at the classical level of significance (against the null hypothesis of no effect for the model's variables, the probability of a greater F-statistic is 0.003 < 0.01).[153]

[152] Thus, the present value of an organization's benefits in 2017 is $PVbnft_{2017} = \sum_{t=1998}^{2017} benefit_t \times (1.07)^{2017-t}$.

[153] The model uses ordinary least squares to estimate, as a function of the sector or sectors of the economy and the type of respondent, the present value in 2017 of a respondent's cumulated benefits over the years: $PVbnft_{2017} = f($sector effects, respondent type effects) with the public administration sector effect (NAICS sector 92) and the public agency respondent effect left in the intercept and with fitted effects for the remaining sectors (NAICS sectors Construction, 23; Manufacturing, 31-33; Retail trade, 44-45;

The third step was to use the estimated model to predict the benefits for the 95 respondents that did not provide enough information to construct any of the benefits shown in Table 5-3 in the body of this report but did provide the information for the variables used in the estimated model of benefits. Namely, for these additional 95 observations, the type of respondent (private consumer, private producer/developer, private integrator, public consumer, academic or independent cryptographer, and cryptographic testing consultant) and its industrial classification were reported. The predicted benefits for these additional 95 respondents are added to the benefits for the 74 respondents to produce an estimate of the benefits for 169 observations.

### Second-Stage Extrapolation Procedure for Estimating Sector-Wide Economic Benefits of 169 Survey Respondents

The extrapolation of benefits to whole sectors of the economy began with a data set for all 169 (74 + 95) survey respondents where their industrial classifications and their types were known. Added to that data set was the number of employees for each respondent's organization if it was reported. For any respondents that did not report the number of employees, it was estimated with the average of the reported employment for respondents of the same type. More elaborate estimates are precluded by the paucity of the data for the set of 95 respondents.

The 169 respondents are distributed across the broad sectors of the economy as shown in Table 5-4, column 1, of the report. Extrapolations of benefits to the sector or broad industry level are developed where ten or more respondents have activity in that category, in order to make the projections to the sector level based on coverage of a more substantial amount of a sector's economic activity. Thus, an extrapolation of benefits for the following sectors is provided, with the number, *n*, of respondents used to make the extrapolation shown in parentheses: Manufacturing (*n* = 45), Information (*n* = 47),

Information, 51; Finance and insurance, 52; Professional, scientific, and technical services, 54; Educational services, 61; Health care and social assistance, 62; Arts, entertainment, and recreation, 71) for which we have observations among the 74 respondents, and for the remaining respondent types (private consumers, private producer/developer, private integrator, and the combined academic/consultant categories). Not unexpectedly given the relatively small number of observations and relatively large number of effects fitted, many of the individual effects estimated are not significant statistically, but the F-statistic for their collective significance is statistically significant: n = 74, F(13, 60) = 2.83, probability of a greater F statistic = 0.0031, $R^2$ = 0.38.

Finance and insurance (*n* = 42), Professional, scientific, and technical services (*n* = 41), Educational services (*n* = 12), Health care and social assistance (*n* = 13), and Public administration (*n* = 16).

Many respondents have activity in more than one sector of the economy.  For each respondent, a variable *z* was calculated that equals the number of different sectors in which the respondent operated. Each respondent's cumulative benefits (*PVbnft2017*—the cumulated value at the social rate of return of its annual benefits over the years) was divided by *z* to have for each of the *n* respondents, the portion of their benefits to be assigned to each of the sectors where they operate.  Note also that within different parts of a sector—the manufacturing sector is a notable example—some respondents are consumers of cryptographic products and services, and some respondents are producers of the products and services.

Report Table 5-4 shows the extrapolation of AES benefits to sectors of the economy where there are ten or more respondents with estimated benefits.