NIST Advanced Encryption Standard (AES) Program Economic Impact Study

Introduction

Introduction

OMB Control No. 0693-0033

Expiration Date: 06/30/2019

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 <stacey.ferris@rmadvisory.com> and Mr. David Leech <david.leech@starpower.net>.

____

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: (301) 975-8530.

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:

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

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?

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$)

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)

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 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	Blowfish Camellia CAST-256 CRYPTON DEAL DFC E2 FROG HPC IDEA LOKI97 MAGENTA MARS Proprietary algorithms RC5 RC6 SAFER+ SAFER K-128 Serpent SQUARE 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$)

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

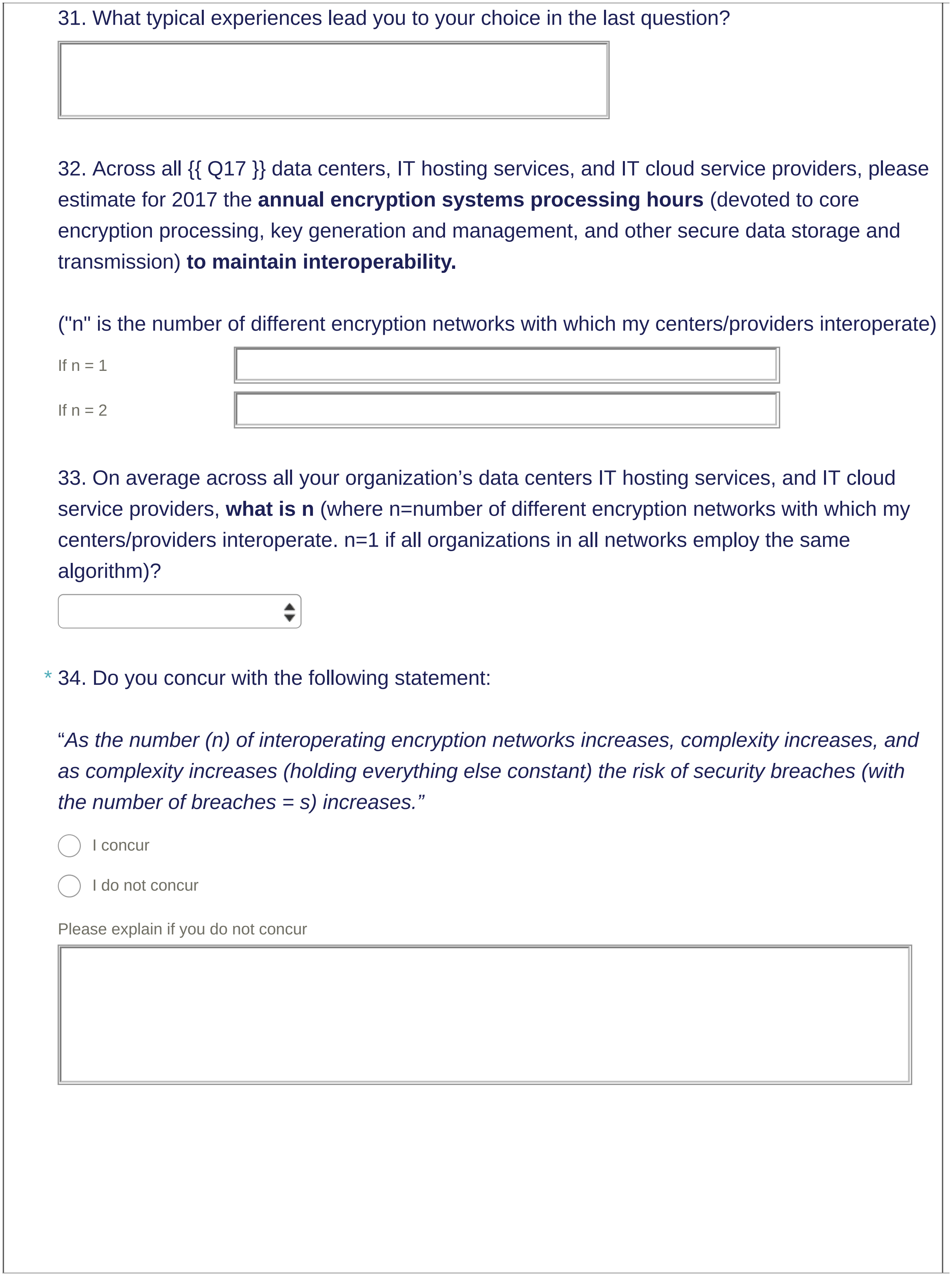
○ Costs to maintain interoperability decline linearly as a function of n

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

○ s remains unchanged as a function of n

○ s declines linearly as a function of n

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

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$)

Private Sector Consumer Part 5 of 5 - Standards Development

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

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:

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

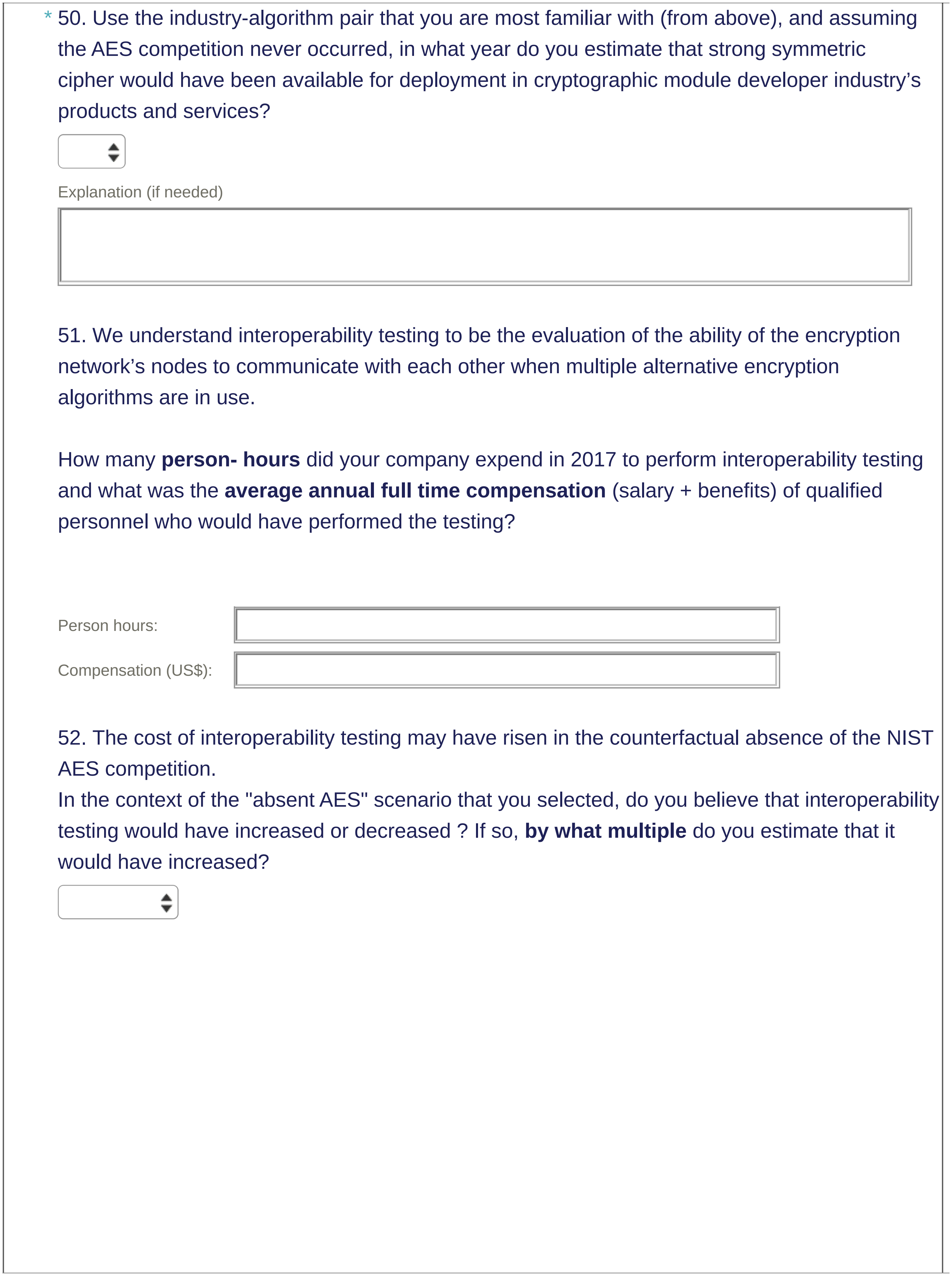
○ E - None of the above. Please explain.

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 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	Blowfish Camellia CAST-256 CRYPTON DEAL DFC E2 FROG HPC IDEA LOKI97 MAGENTA MARS Proprietary algorithms RC5 RC6 SAFER+ SAFER K-128 Serpent SQUARE 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?

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