NIST Generic Clearance for Program Evaluation Data Collections
OMB Control #0693-0033
Expiration Date: 06/30/2019

NIST Advanced Encryption Standard (AES) Program Economic Impact Study

FOUR STANDARD SURVEY QUESTIONS

1. Explain who will be surveyed and why the group is appropriate to survey.

The National Institute of Standards and Technology (NIST) has conducted numerous retrospective economic impact assessments over the years. For examples of such assessments, go to: <https://www.nist.gov/standardsgov/resources/publications#impact> and <https://www.nist.gov/tpo/nist-economic-impact-studies>.

NIST's Technology Partnership Office (TPO) is conducting an economic impact assessment of the Advanced Encryption Standard (AES), Federal Information Processing Standard, FIPS-197. The study period is 1997-2017. The Computer Security Division (CSD) of NIST's Information Technology Laboratory (ITL) has managed the AES program.

The likely beneficiaries of FIPS-197 fall into two broad groups: *consumers* of information encryption systems (i.e., information processing hardware and software used to perform core encryption processing, key generation, key management, and other secure data storage and transmission activities) and *developers* of information encryption systems.

We distinguish between two groups of encryption system *consumers* because the range of choices available to them, with respect to the purchase of encryption system hardware and software, are different and, therefore, the consequence of their choices have different economic effects. The subgroups are *public sector* and *private sector* consumers of information encryption systems.

For the purposes of this survey, *public sector consumers* include the Chief Information Security Officers (CISOs) of Federal agencies and 52 States and territories. *Private sector consumers* include the CISOs (or Chief Information Officers (CIOs), or data center managers) of private sector firms with activities that have to an increasing extent included all sectors of the economy but have historically been concentrated in the R&D-intensive manufacturing sector, and in the financial, medical, and e-commerce service sectors. Professional cyber-security associations whose members include private sector CISOs prominently have been invited to participate in the AES economic impacts survey. They include:

- Accredited Standards Committee X9 (ASC X9, Inc.) (confirmed)
- APWG (formerly, the Anti-Phishing Working Group) (confirmed)
- College of Healthcare Information Management Executives (CHIME) (confirmed)
- Credit Union Information Security Professional Association (CIUSP)
- Evanta-CISO

- Executive Women's Forum on Information Security (EWF)
- Information Systems Audit and Control Association (ISACA)
- Information Systems Security Association (ISSA) (confirmed)
- Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802) (confirmed)
- InterNational Committee for Information Technology Standards (INCITS)
- Internet Security Alliance
- National Council of ISACs (NCI) (confirmed)
- National Cyber Security Alliance
- National Technology Security Coalition (NTSC) (confirmed).

Together, these organizations represent a few thousand potential survey respondents from a wide array of industries. (For purposes of "burden calculation" only confirmed cyber-security associations are included.)

We hypothesize that the benefits that have accrued to *public sector consumers* of AES-based encryption systems include: efficiencies in encryption system processing time due to the performance characteristics of the AES relative to alternative encryption algorithms; associated cost-avoidances (in terms of additional facilities, equipment, and personnel needed to compensate for the reduced efficiency of non-AES encryption algorithms); reduced search costs, qualification costs, and acceptance costs that would have be incurred by user organizations in the absence of a single strong encryption standard; and the costs associated with the delay in standards that have relied upon the AES standard (both the direct costs of developing related standards, and the indirect cost associated with the value-added from delayed sales). It is hypothesized that *private sector consumers* have enjoy additional kinds of benefits, over and above those that have accrued to public sector consumers. *Private sector consumers* of AES-based information encryption systems have also enjoyed benefits associated with increased interoperability. In the absence of the AES, private sector firms could have employed a variety of alternative encryption algorithms, resulting in a variety of encryption networks and increased interoperability costs. Furthermore, it is hypothesized that a decrease in interoperability among private sector consumers of various encryption systems would have increased the complexity of information security systems and, thereby, raised the risk of data breaches among private sector firms.

Turning to *encryption system developers*, for the purposes of this survey *developers* constitute a survey sub-population enjoying a subset of the benefits that are hypothesized to accrue to public and private sector consumers of the information encryption systems. Currently, all Federal agencies require that hardware and software devoted to information encryption utilize a validated implementation of AES (FIPS-197) or Triple-DES (FIPS-46-3) in accordance with FIPS-140-2, the Cryptographic Module Validation Program (CMVP).

Encryption system *developers* to be surveyed include companies that have received or currently maintain cryptographic hardware and software validation certificates (as well as the validation testing consultants and academic or independent cryptographers they employ); and information system integrators of cryptographic modules into hardware and software products available for sale to public and private encryption system consumers. Approximately 1,000 CMVP certificate

holders will be surveyed, representing a mix of companies holding a disproportionate number of all hardware and software certificates currently and historically. (The CMVP maintains a detailed list of current and historical certificate holders, including points-of-contact.)

The benefits that accrue to encryption system *developers* due to AES include: interoperability testing cost-avoidance, internal validation testing cost-avoidance, and transaction cost-avoidance (including potentially costly product recalls). Furthermore, we hypothesize that, like their consumer counterparts, *developers* have avoided direct costs associated with the delay in the development of international standards dependent on AES (costs associated with the standards consensus-making process) and indirect costs associated with increased time-to-market for standardized products and services.

2. Explain how the survey was developed including consultation with interested parties, pre-testing, and responses to suggestions for improvement.

The survey was developed by an experienced contractor team (RM Advisory Services) in consultation with the TPO project lead, Kathleen McTigue. The RM Advisory team includes an expert technical consultant, Dr. Eric Burger, of Georgetown University, an expert economic consultant, Dr. John Scott, of Dartmouth College, and an experienced economic impact project team leader, David Leech. Dr. Scott and Mr. Leech have conducted numerous similar impact assessments for NIST.

In preparation for the design of the survey strategy, an extensive literature survey was undertaken and scoping interviews were conducted with current and former ITL/CSD personnel and nine private sector encryption developers and users. On the basis of this background information, economic impact hypotheses were developed (Attached) that identify the nature of the economic benefits hypothesized for different groups of respondents (discussed in the response to Question 1), the time periods over which the benefits likely occurred, and the alternative approaches to cryptographic security that would likely have been available to public and private consumers in the absence of the Advanced Encryption Standard initiative.

For survey instrument development purposes, the economic hypotheses were expressed in terms of quantities of resources, and the timing of events, to be estimated by CISOs and cryptographic module developers. Survey questions were organized according to the subgroup of the respondents — public or private encryption system users or developers — then sequenced appropriately and formulated in language familiar to CISOs or developers. An on-line survey tool (Survey Monkey) was used to format questions and, where possible, provide drop-down menus and prepopulated question intended to make the survey respondents' experience as easy as possible.

Several of the interviewees engaged during the scoping phase of the project volunteered to beta-test the survey. They were provided with instructions, a survey URL, and a deadline for submissions. On the basis of their critiques the wording of several questions was tightened and some additional answer options were provided.

Given the information demands of survey questions that inform economic impact estimates, we are confident that the attached survey balances the need for essential information against the desire to reduce survey burden and encourage survey response.

3. Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.

The study being undertaken is a case study, not a statistical analysis aimed at generating formal large sample statistical population estimates. While we will use statistics to characterize, and possibly explore survey data, we do not intend to make claims about the statistical accuracy of the estimates of economic impact. This is standard practice for the assessment of the economic impacts of NIST programs.[1] That said, the number of survey responses will be monitored and actions will be taken (described below) to augment the number of survey responses.

The RM Advisory Services project team will utilize a Survey Monkey survey tool and platform to conduct the survey. Selected groups of encryption system consumers and producers will be invited and encouraged to engage in the survey process and a URL link will be provided. Some potential respondents will be contacted directly while others will be invited to participate through their industry association or standards development organization (SDO). Federal and State CISOs will be contacted directly as will validated cryptographic module developers. NIST estimates the number of respondents to be 3000. Each survey taken is estimated to take 35 minutes to complete. NIST anticipates that the overall response rate from direct and indirect survey invitations will be ten percent (10%). Invitations to participate in the survey — direct and indirect — will include the following message:

> *The Technology Partnership Office (TPO) of the National Institute of Standards and Technology (NIST) is conducting a retrospective economic impact assessment of NIST's Advanced Encryption Standard (AES) program (1996-2017). The survey and analysis is being conducted by RM Advisory Services on NIST's behalf.*
>
> *Economic impact assessments demonstrate the effectiveness of NIST programs in terms that budget-conscious stakeholders understand (return-on-investment) and are a source of program management "lessons-learned." Your response will help NIST improve its industry-supporting programs going forward.*
>
> *If you value NIST's contributions to the nation's (indeed, the world's) information security infrastructure, please take the time to respond. 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.*
>
> *The survey will take approximately 35 minutes to complete. To begin, click on the* <https://www.research.net/r/NIST_AES_survey> *link below. We hope to have your completed*

1 See Gregory Tassey, *Methods for Assessing the Economics Impacts of Government R&D*, NIST Planning Report 03-01, National Institute for Standards and Technology, 2003; and Albert Link and John Scott, *The Theory and Practice of Public-Sec tor R&D Economic Impact Analysis,* NIST Planning Report 11-1, National Institute for Standards and Technology, 2012.

response not later than March 30, 2018.

Thank you in advance for your support,

The Survey Monkey survey tool monitors the number of responses. A "respond by" date will be specified in the initial survey invitation. Within two weeks, one week, and two days of that date a "reminder" notification will be sent to non-respondents. Weekly reminders will be sent thereafter with "final response date" notifications sent to the tardiest respondents. Experience indicates that this process *does* marginally improve the number of respondents. The Survey Monkey tool also indicates the degree of completion for each survey response. If respondents submit incomplete surveys *and* provide contact information to allow follow-up questions, they will be encouraged to provide fuller responses.

A similar approach will be taken with indirect respondents — those invited through industry associations or SDOs — but the frequency of the reminders will not be within the project teams unilateral control.

4. Describe how the results of the survey will be analyzed and used to generalize the results to the entire customer population.

We anticipate conservatively that, overall, 10% of those contacted directly and indirectly will respond. In order to scale those responses to the whole population that each subgroup represents, the survey will be augmented with research into the size distribution of organizations within each subgroup. Survey respondents are asked to identify the type of organization to which they belong — public sector consumer (Federal/State), private sector consumer, or cryptographic module/system integrator — and the size of their organization in terms of the number of full-time employees. For public sector respondents, the scaling is straightforward: the ranges of responses from similarly sized agencies that do respond will be assigned to non-responding agencies. For cryptographic module developers, too, the scaling is straightforward: for companies of similar sizes, producing similar hardware or software products in the time periods that estimated benefits occur, the ranges of responses from responding developers will be assigned to non-responding developers. (Historical CMVP certification data identifies certified developers by year of certification and product type. Depending on the number of companies involved, either a historical estimate of individual company size will be ascertained by open source research or an average number of companies of a comparable size operating in the relevant industries will be determined on the basis of historical U.S. Census Bureau data and survey results will be scaled accordingly. The *Annual Survey of Manufactures* provides the number of establishments by employment size categories at the NAICS 6-digit level. The annual *Business Expenses* report provides similar data for the non-manufacturing sector. Comparable data from the Organization for Economic Co-operation and Development (OECD) will be consulted if required.)

Scaling the responses of private sector consumers of information encryption systems, and hardware and software cryptographic module integrators — the total number of which is unknown — will follow the procedure just described as one option for scaling the results

responding cryptographic module developers to the known universe of all certified module developers: for companies of similar sizes, providing similar services or producing similar hardware or software products for the time periods that estimated benefits occur, the estimate ranges of impact value from survey respondents will be scaled up to reflect the total number of consumers and integrators based on available industry statistics concerning the numbers of firms of similar size in their respective industries.

As stated in the response to Question #3, the study being undertaken is a case study, not a statistical analysis aimed at generating formal large sample statistical population estimates. Nevertheless, where opportunities arise, statistical analysis will be employed. For example, in a previous impact assessment by NIST's Standards Coordination Office (SCO), respondents provided sufficient information so that the study team was able to discern statistically valid differences among different groups of respondents. The statistical techniques employed did not depend on the properties of large-sample estimators or statistical normality.[2] We will take advantage of similar opportunities if they arise in the course of the AES impact survey. Respondents are asked to differentiate themselves on a number of dimensions including, for example, respondent category, Federal agency, State, industry sector, SDO participation, size, and longevity of AES use. If a sufficient number of responses are forthcoming in these categories it may be possible to identify interesting differences in the nature or the extent of the economic impacts of AES.

2 See David Leech & John Scott, "Nanotechnology Documentary Standards," *The Journal of Technology Transfer*, Vol. 42, No. 1, 2017, pp. 93-94.