

Supporting Statement for Paperwork Reduction Act Submissions

Title: COVID-19 Contact Tracing Reporting Form

OMB Control Number: 1670-NEW

A. Justification

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.

The Cybersecurity and Infrastructure Security Act of 2018 (the Act) created the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security. Section 2202 (e) (c) of the Act directs CISA to “integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.” With the advent of the global COVID-19 pandemic, the agency has extended our operating environment to include threats to critical infrastructure posed by this biologic threat. Digital contact tracing tools (DCTT) provide both a means to deal and track the spread of the virus, but can at the same time, pose real cybersecurity and other threats to critical infrastructure.

In response to the enduring nature of the pandemic, state, local, tribal and territorial (SLTT) governments and owners and operators of critical infrastructure, have been developing, promoting, and using various forms digital contact tracing tools as a key part of their virus response. However, this is the first use of these digital tools at a large scale or for the purposes of contact tracing. This novel use of existing technology paired with the federal nature of the United States creates a patchwork of digital contact tracing programs and tools that use different means, have different security, and collect different information. To help provide order to this issue and best practices on how to employ these new technologies, CISA needs to know what digital contact tracing tools these entities are employing. Many SLTT governments have already employed or are considering employing a digital contact tracing tool. CISA needs additional back-end development information, which can only be done through a survey, on the type of contact tracing tool used in order to provide cybersecurity and best practices for the large and varied digital contact tracing landscape.

As part of our routine monitoring of our programs, we have seen reports on the cybersecurity issues present in some contact tracing applications that could put millions of Americans’ data at risk. The proposed collection will not attempt to solve all these cybersecurity risks but represents an important first step in better understanding the vulnerabilities and mitigation options needed

to conduct a safe digital contact tracing campaign in order to provide best practices for the public for the most popular types of tools used by stakeholders.

This collection is designed to allow affected parties to voluntarily submit relevant evidence about their contact tracing program. The information will allow the agency to develop best practices and guidance on how to employ digital contact tracing tools while mitigating security risks.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

The COVID-19 Contact Tracing Reporting Form is a voluntary form that CISA will advertise through our Regional Offices and during our frequent engagements with our stakeholders.

CISA will utilize this information on three focus areas:

1. **Contact Tracing Applications:** CISA will conduct an analysis of the cybersecurity policies and practices built into contact tracing applications and tools; catalog emerging solutions and capabilities for contact tracing; and, identify best practices for contract tracing apps and considerations to ensure proper cybersecurity risk mitigation throughout the decision-making process.
2. **Critical Infrastructure Approaches:** CISA will identify how various industry sectors are implementing contact tracing for their workforces or supporting such efforts by local authorities.
3. **State and Local Approaches:** CISA will identify how various State and local governments are implementing contact tracing processes and procedures; note the differences between State and local contact tracing programs and compare against Federal guidance; and analyze opening of non-essential businesses and contact tracing policies to understand differing pandemic risk landscape and conditions across the Nation. This will enable CISA to share best practices for contact tracing programs across the SLTT landscape; provide vulnerability mitigation insights on contact tracing applications; and to work with the Centers for Disease Control and Prevention (CDC) on additional program guidance if warranted.

The Agency will not use information collected through this voluntary feedback collection as the justification for new regulations or policies.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

This information will be collected from a form electronically sent by CISA staff. Respondents will need to fill out the form and submit via email.

4. Describe efforts to identify duplication. In Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

A search of reginfo.gov revealed that this information is not collected in any form, and therefore is not duplicated elsewhere.

5. If the collection of information impacts small businesses or other small entities (Item 5 of OMB Form 83-I), describe any methods used to minimize.

This collection will not impact small businesses or other small entities.

6. Describe the consequence to Federal/DHS program or policy activities if the collection of information is not conducted, or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

As our Nation's risk manager, CISA must undertake efforts to both understand and advise on risks to the Nation's critical infrastructure, to include providing advice and considerations for risk mitigation procedures for State and local governments and owner operators of critical infrastructure engaged in contact tracing due to the possible consequences of failure. As such, CISA must be prepared to address contract tracing to support risk management decisions of our state, local, tribal, territorial, and critical infrastructure partners.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

- (a) Requiring respondents to report information to the agency more often than quarterly.
- (b) Requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it.
- (c) Requiring respondents to submit more than an original and two copies of any document.
- (d) Requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years.
- (e) In connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study.
- (f) Requiring the use of a statistical data classification that has not been reviewed and approved by OMB.
- (g) That includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are

consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use.

- (h) Requiring respondents to submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

The special circumstances contained in item 7 of the Supporting Statement are not applicable to this information collection.

8. Federal Register Notice:

- a. Provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.
- b. Describe efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.
- c. Describe consultations with representatives of those from whom information is to be obtained or those who must compile records. Consultation should occur at least once every three years, even if the collection of information activities is the same as in prior periods. There may be circumstances that may preclude consultation in a specific situation. These circumstances should be explained.

	Date of Publication	Volume #	Number #	Page #	Comments Addressed
<i>60-Day Federal Register Notice:</i>					
<i>30-Day Federal Register Notice</i>					

CISA is seeking an approval of this information collection through the Emergency Approval Process. Upon approval, CISA will follow the normal clearance process and seek public comment through the publication of a 60- and 30-Day Federal Register Notice.

- 9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.**

There is no offer of monetary or material value for this information collection.

- 10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.**

There are no assurances of confidentiality.

This collection is covered by DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups and DHS/ALL-002 DHS Mailing and Other Lists SORN.

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private. This justification should include the reasons why the agency considers the questions necessary, the specific uses to be made of the information, the explanation to be given to persons from whom the information is requested, and any steps to be taken to obtain their consent.

There are no questions of a sensitive nature.

12. Provide estimates of the hour burden of the collection of information. The statement should:

- a. Indicate the number of respondents, frequency of response, annual hour burden, and an explanation of how the burden was estimated. Unless directed to do so, agencies should not conduct special surveys to obtain information on which to base hour burden estimates. Consultation with a sample (fewer than 10) of potential respondents is desired. If the hour burden on respondents is expected to vary widely because of differences in activity, size, or complexity, show the range of estimated hour burden, and explain the reasons for the variance. Generally, estimates should not include burden hours for customary and usual business practices.

To estimate the burden associated with this collection, CISA multiplies the number of responses and the estimated time needed to respond. Based on subject matter expert elicitation, CISA estimates that there will be approximately 166 total submissions. Sixty of the responses will be from SLTT stakeholder and 106 from private sector stakeholders. Each submission is estimated to take approximately 40 minutes. To estimate the total compensation rate for each set of respondents, the average hourly wage is multiplied by a benefits multiplier of 1.425.¹ The SLTT respondent's average hourly compensation rate of \$40.88 is based on an average hourly wage rate of \$28.68² multiplied by 1.425. The private sector average hourly compensation rate of \$35.92 is based on an average hourly wage rate of \$25.20³ multiplied by 1.425. To estimate the cost, we apply a fully loaded hourly compensation rates for each population to the time required to file a submission.

¹ BLS. Employer Costs for Employee Compensation – March 2020. Table 1. Employer Costs per Hour Worked for Employee Compensation and Costs as a Percent of Total Compensation: Civilian Workers, by Major Occupational and Industry Group, December 2019. <https://www.bls.gov/news.release/pdf/ecec.pdf> The compensation factor (1.425) is estimated by dividing total compensation (\$34.73) by wages and salaries (\$24.36).

² Bureau of Labor Statistics (BLS). Occupational Employment Statistics. May 2019. Federal, state, and local government, including government-owned schools and hospitals and the U.S. Postal Service, All Occupations (SOC 00-0000). <https://www.bls.gov/oes/2019/may/999001.htm#00-0000>

³ Bureau of Labor Statistics (BLS). Occupational Employment Statistics. May 2019. Cross Industry, Private Ownership Only, All Occupations (SOC 00-0000). <https://www.bls.gov/oes/2019/may/000001.htm>

As shown in Table 2, the estimated cost associated with reporting is \$4,173.

Type of Respondent	Number of Respondents	Responses per Respondent	Average Burden per Response (in hours)	Total Annual Burden (in hours)	Average Hourly Wage Rate	Total Cost
SLTT	60	1	0.67	40	\$40.88	\$1,635.09
Private Sector	106	1	0.67	71	\$35.92	\$2,538.15
Total	166			111		\$4,173.24

13. Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14.)

There are no recordkeeping, capital, start-up, or maintenance costs associated with this information collection.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing and support staff), and any other expense that would have been incurred without this collection of information. You may also aggregate cost estimates for Items 12, 13, and 14 in a single table.

CISA estimates the burden on the government of this collection by estimating the time required for CISA personnel to review the submissions. All reports will be reviewed by a GS-14. The burden of the GS labor is estimated by multiplying the fully loaded hourly compensation rate of the employee by the number of hours to review. CISA estimates it will take 15 minutes for each review. The hourly rate for a GS-14, Step 3 is \$66.10⁴, which is multiplied by the load factor of 1.425 for a loaded compensation rate of \$94.21. As shown in Table 3 the estimated cost to the Federal Government is \$3,909.86.

Table 3: Government Burden

⁴ GS pay rates are from The annual salary for a GS-14 Step 3 is \$137,491, which is divided by 2080 to obtain the hourly rate. <https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/20Tables/html/DCB.aspx>

Cost Category	Number of Respondents	Responses per Respondent	Average Burden per Response (in hours)	Total Annual Burden (in hours)	Average Hourly Wage Rate	Total Cost
GS-14	166	1	0.25	41.5	\$94.21	\$3,909.86

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I. Changes in hour burden, i.e., program changes or adjustments made to annual reporting and recordkeeping **hour** and **cost** burden. A program change is the result of deliberate Federal government action. All new collections and any subsequent revisions of existing collections (e.g., the addition or deletion of questions) are recorded as program changes. An adjustment is a change that is not the result of a deliberate Federal government action. These changes that result from new estimates or actions not controllable by the Federal government are recorded as adjustments.

This is a **NEW** collection.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

CISA does not intend to employ the use of statistics or the publication thereof for this information collection.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain reasons that display would be inappropriate.

CISA will display the expiration date for OMB approval of this information collection.

18. Explain each exception to the certification statement identified in Item 19 “Certification for Paperwork Reduction Act Submissions,” of OMB Form 83-I.

CISA does not request an exception to the certification of this information collection.