U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Infrastructure Security Division
Washington, DC 20528

26 October 2020

ACTION MEMORANDUM

MEMORANDUM FOR: The Honorable Paul Ray
Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget

THROUGH: The Honorable Karen S. Evans
Chief Information Officer
Department of Homeland Security
ELIZABETH A CAPPELLO
Digitally signed by ELIZABETH A CAPPELLO
Date: 2020.10.28 15:34:26 -04'00'

FROM: Scott Breor
Deputy Assistant Director (Acting)
Cybersecurity and Infrastructure Security Agency (CISA)
Infrastructure Security Division
SCOTT F BREOR
Digitally signed by SCOTT F BREOR
Date: 2020.10.23 15:59:09 -04'00'

SUBJECT: Emergency Information Collection Request (ICR): An Evaluation of Contact Tracing for Critical Infrastructure Owners, and State and Local Partners

---

Purpose: The memorandum seeks approval from Office of Management and Budget (OMB) of the U.S. Department of Homeland Security (DHS) emergency review request under the Paperwork Reduction Act (PRA) to collect information from critical infrastructure owners, and State and local partners on digital contact tracing approaches and tools being used in response to the COVID-19 pandemic.

Background: On April 16, 2020, the White House issued "Opening Up America Again," a set of Federal guidelines for reopening the US economy with a three-phased approach. One core State preparedness responsibility is the need for contact tracing of individuals who test positive for, or are symptomatic of, COVID-19. Digital Contact Tracing Tool (DCTT) applications if not properly secured can pose a great threat to the privacy, the personally identifiable information (PII), and personal health information (PHI) of individuals and can pose an equal threat to the computer systems of those operating those tools. CISA under the Cybersecurity Information Sharing Act of 2015 and the Homeland Security Act, "is to provide best practices and 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." CISA cannot advise on DCTT currently due to the patchwork nature of state and business adoption of DCTT technologies and the lack of public information available on the many DCTT applications. It is imperative that cybersecurity best practices on the employment of these new technologies be out while the use of DCTT is still nascent.

Discussion: While there is some general information about how states and local governments and owner/operators of critical infrastructure plan to implement contact tracing; specific information on applications is lacking. Due to this gap in actionable information, CISA determined that it is necessary to collect additional data in order to formulate risk mitigation measures. CISA explored other options for obtaining this data and found that the information is not available without invoking the PRA. CISA determined that the most efficient way to obtain the needed information is by soliciting direct feedback from owners of critical infrastructure, and State and local partners. Considering the reoccurring COVID-19 hotspots and possibility of a second wave of infections, CISA is seeking emergency clearance to include additional questions, outlined in the attached documents, for this outreach. CISA will use the findings to develop best practices and considerations for cybersecurity risk mitigation procedures for the contact tracing applications and tools.

Without emergency approval, CISA will be unable to collect the required information in order to assist critical infrastructure owners, and our State and local partners at the early stages of their contact tracing activities by advising on critical cybersecurity threats and sharing CISA best practices. In turn, nefarious actors could exploit vulnerabilities and threaten the personal identifiable information and personal health information of millions of Americans. Although CISA regularly informs the public of cybersecurity threats and on best practices on cybersecurity, the breadth of possible DCTT an organization could use made by innumerable vendors would make general advice unhelpful. By collecting this information CISA will be able to tailor best practices to the DCTT that are actually being used by stakeholders, rather than providing general advice that may not apply actually mitigate known cybersecurity risks.

Estimated Timeline:

1. Survey implementation needs to be initiated as soon as possible due to the number of digital contact tracing tools being implemented across the nation.

2. Analysis of the survey/data will last 2 weeks, and the assessment for the identification of risk management solutions will generally take another 2 weeks to prepare.

3. OMB should approve the survey by November 5, 2020 in order for CISA to meet the planned schedule timeframes for the deployment of risk mitigation solutions.

Conclusion: CISA respectfully requests that OMB grant DHS's request for emergency clearance to conduct outreach and receive information in order to provide advice and considerations for risk mitigation procedures.

Approve/date_____ Disapprove/date_____

Modify/date _____ Needs discussion/date_____

Attachments:

1. 1670-NEW_COVID-19 Contact Tracing Reporting Form_1_SSA_v2
2. 1670-NEW_COVID-19 Contact Tracing Reporting Form_3_FORM-v2
3. 1670-NEW_COVID-19 Contact Tracing Reporting Form_4_20200730_PTA-v2