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

ACTION MEMORANDUM

MEMORANDUM FOR: Sharon Block
Acting Administrator
Office of Information and Regulatory Affairs
Office of Management and Budget

THROUGH: Eric Hyson
Chief Information Officer
Department of Homeland Security
ERIC N HYSEN Digitally signed by ERIC N HYSEN Date: 2021.06.23 08:54:49 -04'00'

FROM: Kevin Dillon
Associate Director
KEVIN E DILLON Digitally signed by KEVIN E DILLON Date: 2021.06.17 16:26:05 -04'00'
Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency

SUBJECT: **Emergency Information Collection Request (ICR): State, Local, Tribal and Territorial Incident Collection**

Purpose:
As requested, please find this justification memorandum for emergency clearance of the Cybersecurity and Infrastructure Security Agency's (CISA) request for emergency review under the Paperwork Reduction Act (PRA) to complete OMB Control Number 1670-NEW "State, Local, Tribal and Territorial Incident Collection Form" (the "Form").

There has been a quantifiable increase in scams and malicious activity with themes related to our nation's critical infrastructure and Coronavirus Disease 2019 (COVID-19). Malicious cyber actors are targeting individuals, small businesses, State, Local, Tribal and Territorial (SLTT) governments, and other entities with COVID-19-related scams, ransomware and phishing campaigns. There has also been an increase in attacks, including using ransomware, related to critical infrastructure. This includes the attack on a water treatment facility managed by a local government agency that impacted the safety of drinking water for an entire community, the Colonial Pipeline ransomware attack that for days halted fuel distribution from a crucial pipeline on the East Coast of the United States, and the ransomware attack on a critical meat processing company. Although these instances made national news, CISA knows that most cyber incidents go unreported, which is why we are exploring ways to increase reporting through the Form. Currently the pilot includes five states, and only one of which has a current statewide form. The Form will provide a way to identify potential crimes so that law enforcement can take action and for CISA, it will provide critical information on the scope and scale of attacks, not to mention changes in

tactics by malicious cyber actors, so that we can adjust our programs in the short-term to help SLTTs address ransomware and more general cybersecurity breaches and issues.

Background: The National Infrastructure Protection Plan (NIPP) 2013 guide DHS in its execution of Presidential Policy Directive 21: Critical Infrastructure and Resilience, which calls on the Federal Government to advance a unified national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. The NIPP identifies 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. These sectors include everything from energy, water, food and agriculture, finance and nuclear infrastructure.

There is currently no standard mechanism for individuals and small businesses to report cyber incidents. A primary result is an incomplete understanding of both the totality of incidents and the tactics, techniques and procedures deployed by malicious cyber actors. To begin to address this gap, CISA launched the SLTT Incident Reporting and Threat Information Sharing Pilot to advance nationwide cyber incident response capabilities and efforts to respond to cyber incidents by standardizing the reporting structure and mechanism. A cooperative agreement was awarded to the Cybercrime Support Network to identify ways to improve individual reporting of cyber incidents and the delivery of assistance to victims. A primary objective is to evaluate methods to standardize reporting structures and mechanisms.

CISA developed the Form as part of a prototype process to voluntarily collect cyber incident information. As the data collection mechanism, the Form provides a secure, standardized, web-enabled means for individuals and small businesses to report cyber incidents. The data collection phase of the pilot is only expected to last for three months and will include up to five states. CISA, through the awardee, will provide detailed incident data to the appropriate state agencies for investigation. More broadly, pilot participants will be provided generalized trend analysis to help them better understand the increased vulnerabilities. CISA will receive both generalized trend analysis and details on the Form's usability. CISA will not receive individual incident reports.

In addition to supporting SLTT agencies and CISA addressing cyber incidents, an added benefit of expedited approval is that lessons learned from the pilot will be incorporated into CISA's standard PRA approval submission in the future. This will make for a much more complete and informed submission.

Federal law enforcement is investigating over 100 different ransomware variants and now considers ransomware attacks as terrorism. Ransomware has the potential to not only disrupt major elements of the U.S. economy but also to cause significant deaths and public harm. Thus, CISA needs this collection method as part of a comprehensive set of tools to gain a better understanding of the ever-changing cyber environment and to protect citizens for harm.

On February 7, 2021, a water treatment plant in Oldsmar, Florida was breached resulting in the intruder opening various software functions that control the water being treated. The intruder boosted the level of sodium hydroxide—or lye—in the water supply to 100 times higher than normal. This attack could have caused massive amounts of deaths in the service area.

The May 7, 2021, ransomware attack on the Colonial Pipeline Company, forcing the company to take some systems offline and disabling the pipeline. The Georgia-based company operates the largest petroleum pipeline in the United States, carrying 2.5 million barrels a day of gasoline, diesel, heating oil, and jet fuel on its 5,500-mile route from Texas to New Jersey. This attack caused massive fuel lines across the south and east coast of the United States and severely limited interstate commerce.

On June 1, 2021, a ransomware attack on the world's largest meat processor forced the shutdown of nine beef plants in the United States which disrupted production of poultry and pork plants. The attack upset the nation's meat markets and raises new questions about the vulnerability of the food infrastructure.

For these reasons, we ask that you approve our request for emergency clearance of the SLTT Incident Collection to provide a valid OMB Control Number for a period of six months.

Thank you for your consideration.

Conclusion: We recommend approval of this request to ensure CISA can collect volunteered information for three months through the Form from individuals and small businesses who believe they have been a victim of a cyber incident.

Attachment(s):

A. 1670 - NEW_SLTT Incident Collection_SSA_v9
B. 1670 - NEW_SLTT Incident Collection_INSTR_v2
C. 1670 - NEW_SLTT Incident Collection_PTA_20200916 FINAL