United States Senate
WASHINGTON, DC 20510

November 18, 2019

The Honorable Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane, Mail Stop 0380
Washington, D.C. 20528-0380

Dear Director Krebs:

We write to you to express our concern about a potential shortfall in funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) and to ask that the Department of Homeland Security (DHS) fully fund these efforts.

We appreciate and value your work to support safeguarding the nation from cyber threats. The Cybersecurity and Infrastructure Security Agency's (CISA) mission of sharing timely and actionable threat information and helping organizations understand their risk profile has never been more critical than it is now as we face increasingly sophisticated threats from criminal organizations and nation states. MS-ISAC and EI-ISAC are vital to the success of this mission.

As you know, State, Local, Territorial and Tribal (SLTT) entities have been consistently targeted by malicious hackers. Recently, across the nation our cities and states have suffered from debilitating ransomware attacks that are carried out to extort public funds.[1] According to a recent report, state and local governments were the targets of 230 attacks from 2013 through the end of September 2019, 81 of them occurring in 2019. Twenty-nine of these attacks targeted school districts with 15 occurring in August and September, timed with the beginning of school year.[2] Local governments – including small towns, counties, and school districts - simply do not have the budgets, the personnel, or the expertise necessary to deploy sophisticated tools in order to defend themselves against this evolving threat environment. There is an urgent need for greater resources and expertise from the federal government to help these entities build their resilience and defenses.

CISA has long relied on partnerships to advance its mission, and the MS-ISAC is a prime example of this partnership-based approach. For nearly a decade, the Center for Internet Security

[1] Adam Meyers, "The Big E-Crime Pivot," May 7, 2019, Dark Reading: https://www.darkreading.com/risk/the-big-e-crime-pivot/a/d-id/1334605

[2] Allan Liska, "Update: New Findings in Ransomware Attacks on State and Local Government", October 8, 2019, Recorded Future blog: https://www.recordedfuture.com/state-local-government-ransomware-attacks-update/

(CIS) has held a cooperative agreement contract with the Department and served as a vital intermediary between SLTT governments and DHS. The ISAC has marshalled threat information, best practices, tools, and expertise to assist SLTT entities with hardening their cybersecurity posture. As threats evolved to target election infrastructure, CIS took on the additional mission of running the EI-ISAC. It has also built the trusted relationships on the ground with the local entities to ensure a free flow of information among SLTT entities and with DHS. Thus far, we have heard overwhelmingly positive feedback from organizations that represent State and local entities about the services CIS and these ISACs provide. These efforts advance the Department's cybersecurity mission.

It is, therefore, surprising and concerning that CIS may not have enough funding to carry out its mission of improving the overall cybersecurity posture of the nation's SLTT entities – the exact mission that CISA has asked it to take on. We were dismayed to learn that the Department's proposed budget for Fiscal Year 2020 covers less than 70 percent of the approximately $15 million required to maintain MS-ISAC and EI-ISAC services at current levels. We urge you to address this funding gap and fund the MS-ISAC and EI-ISAC at the level that does not result in CIS reducing or eliminating their services to their customers.

With the recent surge of ransomware attacks and 2020 elections fast approaching, we cannot afford to curtail support to SLTT entities and election administrators when they need it most. The prospect of a ransomware attack against election infrastructure is real and threatens the foundations of our democracy. We hope that you will work with us to address this urgent concern and ensure that DHS provides MS-ISAC and EI-ISAC with the resources necessary to continue their important mission.

Thank you for your consideration of our request.

Sincerely,

Maggie Hassan
Margaret Wood Hassan
United States Senator

Charles Sch
Charles E. Schumer
United States Senator

Gary C Peters
Gary C. Peters
United States Senator