VERMONT LEAGUE OF CITIES & TOWNS

*Serving and Strengthening Vermont Local Governments*

# MEMO

TO: House Energy and Technology Committee

FROM: Karen Horn, Director Public Policy & Advocacy (khorn@vlct.org)

RE: Municipal Cyber Security Risks Due to COVID-19

DATE: June 9, 2020

The COVID 19 pandemic has fundamentally changed the way that local governments work and their ability to adapt governance in every regard. Most significantly, when the Governor issued his Executive Order 01-20 on March 14, work moved to the internet where on-line communication was an option, and local government was no exception. The transition happened virtually overnight as physical offices and meeting places closed down. Local officials had to transition public meetings, regular work activities, supporting emergency management and public safety, and staying compliant with open meeting and public records laws to virtual platforms. Much of that remote work requires interfacing with state websites, from the Department of Taxes and Motor Vehicles, to the Agency of Natural Resources, Secretary of State's office, and many more.

At the same time, across the globe the transition from face to face work to remote work has created enormous opportunity for cyber criminals to prey on those who are newly engaged in the world of the internet. There are numerous articles that warn against succumbing to cyber criminals' increasingly sophisticated ploys to gain access to vulnerable networks. In short, the wholesale move to on-line business, tele-health, education and governance greatly enhanced the likelihood of falling victim to cyber crime that would jeopardize local government computers, networks, servers and devices.

Local officials need professional assistance to find and assess their cyber security vulnerabilities and to establish a prioritized list of responses to secure their systems. The need is far more acute since the move to remote work places and teleconferencing platforms that in many instances were not used at all before the COVID 19 emergency. Local officials also need on-going awareness training to recognize the endlessly evolving iterations of attempts to breach security in their local systems.

We support language that would provide for the Agency of Digital Services to use CARES Act Coronavirus Relief Fund dollars to hire consultants to support municipal officials in addressing cyber-security risks, assessing and mitigating vulnerabilities posed by closed municipal offices and the transition to remote work and hosting of public meetings in compliance with the open meeting law.

There are approximately 9961 municipal employees and local elected officials who are paid for services according to data from the Department of Labor. We suggest it would cost at least $350,000 to conduct preliminary assessments of vulnerabilities and provide on-going training to spot attempts to breach systems' security.

Thank you for your consideration of this need at the local level.