VLCT TESTIMONY
89 Main Street, Montpelier, Vermont 05602

To: Members of the Joint Information Technology Committee
From: Karen Horn, Director, Public Policy and Advocacy, khorn@vlct.org www.vlct.org
Date: October 18, 2019
Re: Cyber Security in Municipal Government

Thank you for the opportunity to testify on the subject of cybersecurity at the municipal level.

Everyone – businesses, government, individuals – needs to practice constant vigilance to protect digital information. Unfortunately, governments are attractive targets for cybercrime right now. Cities and towns hold significant amounts of sensitive information that cyber criminals want and many of our member municipalities are ill prepared to fend off attacks.

Equipment can be old. Staff across a municipality can click on a phishing message that compromises the entire system. Passwords may be infrequently changed or inadequate. Towns may not have their own domain but rather just a laptop and password.

We also understand that the weakest link in any cyber security system is the human. Criminals gain entry to a system when someone clicks on the wrong link or responds to the wrong email or phone call, when someone is not constantly suspicious of the messages that come their way from any direction. While there have been breaches due to human error at the local level in Vermont, we are not aware at this time of a ransomware attack on a municipality in Vermont. Norwich is the most recent example of a breach of security - due to human error.

VLCT Property and Casualty Insurance Fund (PACIF) insures 348 municipalities ranging from fire districts to public safety authorities (but not schools). Of that total, PACIF insures seven cities, 230 towns (including the Unified Towns and Gores of Essex County) and 22 villages. PACIF introduced Cyber Liability and Data Breach Coverage in 2018 in response to computer security risks created by software-based criminal activities. It covers exposures such as unauthorized disclosure of personal information, cyber extortion, payment card industry penalties, regulatory fines, and loss or corruption of data. PACIF staff are working with Norwich and given the specific nature of the event there, expects to make the town whole for funds they have been unsuccessful in recovering.

We are acutely aware that government leaders need to make cybersecurity an on-going priority for administration, education, testing, and budgeting. We understand that when security breaches expose sensitive information, trust in government at whatever level is likely to erode.

Local officials are clearly concerned about the evolving nature of threats to the safety of their data. A significant part of the issue is that it is confusing to figure out what you need to do to keep staff alert to assaults and keep information safe.

We provide training and make resources available to member cities and towns.

- The keynote speaker at the VLCT annual meeting and Town Fair on October 3, was Morgan Wright, internationally recognized expert on cyber security strategy, cyber terrorism, identity theft and privacy. Jonathan Rajewski, Director of the Senator Patrick Leahy Center for Digital Investigation at Champlain college gave a follow-up workshop, *Practical Cyber Security Advice for Vermont's Cities and Towns* that same day.

- We hosted a webinar with KnowledgeWave this week on Computer Security Awareness.

- Our website has a page dedicated to cyber security including contacts for vendors who will conduct security audits and trainings such as the October 22 cybersecurity training at Champlain College. https://www.vlct.org/cybersecurity

- PACIF members have access to the PACIF On Line University, which trains local officials on a wide range of loss control topics including cyber security.

- The National League of Cities has just issued a new publication to help municipalities, *Protecting Our Data: What Cities Should Know about Cybersecurity*. The publication recommends six strategies for cyber secure cities. It highlights efforts on the part of the states of Georgia, West Virginia, New York and Virginia to help fund local government security measures. Those include identifying one person to be responsible for cyber security; educating the workforce; analyzing vulnerabilities; backing up data; multi-factor authentication; plan for managing potential attacks.

https://www.nlc.org/resource/protecting-our-data-what-cities-should-know-about-cybersecurity

- We have worked with the Department of Taxes as they developed a request for proposal for a new, modern integrated property tax management system that incorporates security measures.

We urge the committee to consider ways in which the legislature and state can help municipalities to protect their data and networks. Funding for on-going training around best practices and upgrading equipment will be most helpful