Cybersecurity Coalition
ALLIANCE FOR DIGITAL INNOVATION
The Software Alliance BSA

CompTIA
CYBER THREAT ALLIANCE
GLOBAL CYBER ALLIANCE
ITI

April 20, 2020

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
H-232, The Capitol
Washington, D.C. 20515

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
H-204, The Capitol
Washington, D.C. 20515

Dear Speaker Pelosi and Leader McCarthy:

The undersigned Coalitions are writing to you to urge the inclusion of dedicated funding to support cybersecurity for State and local governments in the next COVID-19 relief package.

COVID-19 has upended every aspect of American life, including significantly increasing the need to maintain and secure State and local networks, clouds, and end points. These systems provide critical services, particularly as residents increasingly telework, access State resources online, and depend on state and locally-owned and operated critical infrastructure including hospitals. State and local entities, however, have long lacked the resources to adequately secure and maintain their digital infrastructure. The rise in malicious cyberattacks targeting State and local entities, combined with the chronic lack of workforce, patchwork legacy systems, under-resourced cybersecurity and IT services, and uneven federal assistance creates a greater risk of system failures that interrupts services on which State and local populations depend.

2019 saw a significant rise in the number of cyberattacks perpetrated against State and local entities, and this is a trend that appears likely to continue.[1, 2] While high profile cases in Baltimore, New Orleans, and Atlanta grabbed the headlines, there were hundreds of more attacks reported and many hundreds likely unreported or undiscovered.[3] This was the reality before COVID-19. Things have become considerably worse in the months since. Nowhere is this more

[1] https://www.recordedfuture.com/state-local-government-ransomware-attacks-update/
[2] https://www.recordedfuture.com/state-local-government-ransomware-attacks-2019/
[3] Ibid

apparent than among State and locally-owned and operated public hospitals. Healthcare facilities like these, which make up nearly 20% of the United States' community hospitals, have been targeted by malicious cyber attacks at a time when disrupted service is intolerable.[4] [5]

During this unprecedented period, State and local cybersecurity and IT workforces have seen their capacity diminished by health concerns and telework inefficiencies. However, their responsibilities have only grown as they contend with the numerous additional obstacles and vulnerabilities created by the rapid and unexpected adoption of mass telework policies. Additionally, their limited resources risk being overwhelmed by the substantial increase in demand for online services, and the sizeable increase in malicious cyber activities as reported by both State and local officials, as well as private sector threat intelligence organizations.[6]

Telework is a commonality that underlies both the increase in demand for services and the increase in malicious cyber activity. While telework has been rightly praised for its ability to augment healthcare and mitigate damage to the economy, public and private entities alike are now attempting to cope with the numerous, serious threats and vulnerabilities inherent to telework and its rapid, unplanned implementation. These threats and vulnerabilities may include:

- A substantial increase in the use of unvetted personal devices used to access State and local [7]networks and conduct sensitive business;
- Increased use of cloud services and applications that are often not properly secured;
- An increase in the use of unsecured networks;[8]
- A substantial increase in costs associated with providing IT support, cybersecurity, and monitoring of personal devices;[9]
- A substantial increase in the difficulty of ensuring security updates and patches are routinely and uniformly applied;[10]

[4] https://www.aha.org/statistics/fast-facts-us-hospitals

[5] See https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware and https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/15/the-cybersecurity-202-hospitals-face-a-surge-of-cyberattacks-during-the-novel-coronavirus-pandemic/5e95fbc9602ff10d49ae4ba4/ and https://subscriber.politicopro.com/article/2020/04/foreign-governments-hacking-us-labs-and-hospitals-fighting-coronavirus-fbi-official-says-3979469. l

[6] https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/

[7] https://fcw.com/articles/2020/03/22/covid19-federal-response-contractors-tech.aspx

[8] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

[9] https://www.smartcitiesdive.com/news/cybersecurity-risks-spike-as-covid-19-forces-city-staff-to-go-remote/575281/

[10] https://www.us-cert.gov/ncas/alerts/aa20-073a

- Inadequate identity and authentication systems, both for securing government enterprises, as well as for enabling secure delivery of digital services to citizens;
- A lack of trained personnel who can adequately advise on secure telework policies and products (e.g. VPNs, video/audio conferencing) and who can configure and manage appropriate safeguards to telework technologies;
- The loss of physical security controls and enterprise-network related security measures;[11]
- The widespread use of 3rd party telework products that have not been thoroughly tested for cybersecurity vulnerabilities;[12, 13] or
- An increase in malicious actors targeting telework technologies.[14]

Some of these vulnerabilities have been actively exploited and pose significant risks to State and local critical functions and services. As it stands, State and local entities are simply not resourced to effectively address these new challenges over the extended period that pandemic mitigation measures will likely need to remain in place.

It is within this context that the undersigned organizations thank Representatives Thompson, Richmond, Kilmer, and Ruppersberger for their leadership in calling for cybersecurity assistance grants.[15] We urge addressing this important problem in the next available vehicle for COVID-19 response and recovery. We firmly believe that these measures are necessary to support the vital role that State and local entities play in public health operations during this public health emergency, their pivotal role in delivering relief and response services to citizens during these extraordinary times, as well as their role in maintaining the health of the nation's cybersecurity ecosystem.

Sincerely,

Alliance for Digital Innovation
BSA | The Software Alliance
The Computing Technology Industry Association (CompTIA)
Cyber Threat Alliance
Cybersecurity Coalition
Global Cyber Alliance
Information Technology Industry Council (ITI)

[11] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

[12] https://www.cyberscoop.com/zoom-zero-day-webcam-privlege-escalation/

[13] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic/layout_view

[14] https://www.us-cert.gov/ncas/alerts/aa20-073a

[15] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2020/apr/cs2020_0136.pdf