[DRAFT]

The Honorable Nancy Pelosi
H-232, The Capitol
Washington, D.C. 20515

The Honorable Kevin McCarthy
H-204, The Capitol
Washington, D.C. 20515

Dear Speaker Pelosi and Leader McCarthy,

As you work with the committees to develop legislation to address the unprecedented COVID-19 pandemic and ensure the long-term resiliency of our economy, we urge you to include measures to modernize and secure the information technology (IT) infrastructure that state and local governments rely on. In the bipartisan CARES Act, we recognized the vital role states and municipalities are playing on the front lines of this crisis and provided funding both to address COVID-specific needs and to help administer federal programs that are managed by state agencies. However, these investments are insufficient to address the significant technical challenges states continue to face, nor will they address rising cybersecurity concerns as more work is conducted remotely.

The coronavirus pandemic has abruptly revealed how ill-prepared many of our state and local governments are to remotely and securely deliver vital public services to constituents at a large scale. In Oregon, for instance, the decades-old unemployment insurance system has led to waits of five weeks or more to get processed for enhanced benefits provided under the CARES Act.[1] Kentucky, too, has struggled with a legacy unemployment system that has ground processing to a halt.[2] Many states point out that unemployment claims have ballooned extremely rapidly, but in states with modern cloud-based infrastructure, like Rhode Island, systems have been able to relatively easily scale to meet demand.

Antiquated state and local IT systems also place employees at risk. When telework capabilities are not available, essential workers may be exposed to riskier environments to carry out their duties. We are already seeing this as state and local employees go into the office despite stay home orders to process requests that cannot be handled remotely.[3]

As more essential services have moved online due to the CoVID-19 pandemic, they are at increased risk of disruption due to a cybersecurity incident. Security researchers estimate that CoVID-19-related phishing attacks were up 667% in March,[4] and state CISOs have ramped up prevention measures for state systems to defend against cyber intrusions.[5] In fact, cybersecurity training providers from the Texas A&M Engineering Extension Service Cyber Readiness Center, a member of the National

---

[1] https://www.kgw.com/article/news/health/coronavirus/oregon-gov-kate-brown-apologizes-for-unemployment-claim-delays/283-cd93c23f-9f01-4609-86ee-89c4696eb64d

[2] https://www.courier-journal.com/story/news/investigations/readers-watchdog/2020/04/08/kentucky-coronavirus-unemployment-benefit-filing-stresses-call-center/2940019001/

[3] Underfunded, Understaffed, and Under Siege: Unemployment Offices Nationwide are Struggling to Do Their Jobs, Washington Post (April 6, 2020) https://www.washingtonpost.com/business/2020/04/06/unemployment-benefits-coronavirus/

[4] Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020, Security Magazine (April 16, 2020) https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020

[5] How Public Agencies Can Guard Against a New Wave of Phishing Attacks, State Tech Magazine (March 25, 2020) https://statetechmagazine.com/article/2020/03/how-public-agencies-can-guard-against-new-wave-phishing-attacks

Cybersecurity Preparedness Consortium, report a significant increase in course participation from public sector entities since the start of the CoVID-19 pandemic.[6] Increased reliance on technology broadens the attack surface that malicious actors, whether criminals, nation-state adversaries, or hacktivists, can exploit. Unfortunately, legacy IT systems often run on proprietary and no longer supported technologies and are frequently incapable of allowing even relatively unsophisticated cybersecurity controls, such as encryption or multifactor authentication, which can make defending them a serious challenge.

The Cyberspace Solarium Commission,[7] a Congressionally chartered public-private entity charged with developing a national cybersecurity strategy, released its report to Congress on March 11. In it, the commissioners recommend that state, local, tribal, and territorial (SLTT) governments adopt secure cloud services to provide greater flexibility, scalability, and security.[8] The 14 commissioners of the CSC, which included government leaders, academic experts, and business executives steeped in the challenges of securing cyberspace, concluded that cloud service providers enable smaller entities like state and local governments to obtain a level of cybersecurity and functionality that they may not be able to achieve with traditional on-premise systems, making them a foundational element of our digital future.

We strongly support the Solarium Commission's findings and believe that providing an infusion of IT modernization grant funding to states and localities will help them deal with the significant demands being placed on their systems, protect their workers, and improve their cybersecurity posture. When considering how to implement such a recommendation in a COVID relief package, we strongly encourage you to adhere to the following principles:

- *Maximum flexibility for systems eligible to receive funding* – States have varying degrees of maturity across the many systems they maintain. Flexibility ensures that federal support can be used to maximum effect by allowing states to prioritize systems that they judge are at highest risk based on the specific threats to, vulnerabilities in, and consequences of a breach of those systems.
- *Certification baselines and security planning requirements* – Modernization should prioritize a cloud-first approach using vendors that achieve certification against industry-developed standards. However, to ensure mission owners bake security into their proposed modernized architecture, State Chief Information Officers should be required to submit modernization plans using quantized risk assessments to the Cybersecurity and Infrastructure Security Agency for review.
- *Local needs considered* – Local governments are often even more resource-starved than their state counterparts. Any modernization plan should ensure that local governments are able to access a portion of the funding for their needs and that a state will offer shared services to local governments that reflect their needs.
- *Investments for today and for the future* – Many states have immediate IT modernization needs as well as longer term, more meaningful system redesigns. Some portion of funding should be available to meet these immediate equipment and license needs while the bulk is available for

[6] Texas A&M Engineering Extension Service Cyber Readiness Center
[7] https://www.solarium.gov/
[8] See Commission recommendation 4.5.1, Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses, and State, Local, Tribal, and Territorial Governments

more substantive projects that will ensure we can withstand this public health crisis and the resultant economic downturn.

It is important to note that this funding should happen in conjunction with—not in place of—sustained operational proposals such as H.R. 5823, the S*tate and Local Government Cybersecurity Improvement Act*,[9] that would provide $400 million in grants for states to mitigate cybersecurity risks deemed imminent by the Cybersecurity and Infrastructure Security Agency on an annual recurring basis. States maintain systems critical to our country, such as our elections, and they are often the target of sophisticated nation-state hackers. Without federal assistance, states face a major strain on resources when asked to repel persistent threats from adversaries like China's People's Liberation Army or the Russian GRU. H.R. 5823 will help states make the investments necessary to better defend their networks against these advanced persistent threat actors and to improve their resilience; however, *without separate, significant investments in IT modernization, it is very unlikely that states will be able to fully capitalize on these additional resources because their systems will be too old to defend*. We strongly recommend that language similar to H.R. 5823 also be included in a relief package to complement IT modernization efforts and ensure we are best positioned to defend our democracy.

The need for modernization efforts at the state and local level is abundantly clear for both operational and cybersecurity reasons. We also believe that a one-time investment in state and local modernization is good public policy. As demonstrated in the CARES Act, federal policy is often executed through the states, and it relies on IT infrastructure to be delivered effectively. An infusion of federal funding for modernization efforts is also likely to be sustained in the out years as operating costs for modern IT systems are often lower than for legacy systems.

In this new era of increased reliance on IT systems to deliver public services, we urge you to fund state and local IT modernization initiatives as part of future coronavirus-related legislation. These efforts will enable states to rapidly scale up to meet extraordinary demand and reduce vulnerability of their networks. Thank you for your leadership during these unprecedented times and for your consideration of our request.

Sincerely,

[9] https://www.congress.gov/bill/116th-congress/house-bill/5823