The Honorable Mitch McConnell
Majority Leader
United States Senate
317 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Charles E. Schumer
Minority Leader
United States Senate
322 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Richard Shelby
Chairman, Committee on Appropriations
United States Senate
U.S. Capitol, Room S-128
Washington, D.C. 20510

The Honorable Patrick Leahy
Vice Chairman, Committee on Appropriations
United States Senate
U.S. Capitol, Room S-128
Washington, D.C. 20510

Dear Senators,

As you deliberate additional legislation relating to the COVID-19 pandemic, state government information technology (IT) services continue to experience unprecedented demands to ensure the delivery of timely and critical services to citizens and maintain and protect the continuity of government. On behalf of the nation's state chief information officers (CIOs), we greatly appreciate resources provided by Congress in the CARES Act to support state governments. However, we want to highlight additional costs beyond the direct benefits that must be considered as you debate subsequent legislation.

As you know, states are the chief administrator of crucial federal programs and benefits, including benefits provided in the CARES Act. Throughout the past four months of this pandemic, state technology systems, which in normal times are overburdened and under-resourced, have been inundated with significant demands to expeditiously provide benefits such as small business loans, unemployment insurance and other vital services that have become increasingly critical during the pandemic. State IT agencies have reported more than a 2,000% increase in traffic to their unemployment benefits portals, which largely run on outdated legacy infrastructure.

Since the beginning of the COVID-19 pandemic, state IT agencies across the country have admirably risen to the challenge of supporting the delivery of critical services to citizens while 80-90 percent of their workforce quickly moved remotely. State IT agencies, led by state CIOs, have rapidly invested in significant IT infrastructure to support the drastic increase in technological and security demands, but additional resources are clearly needed as the impact of COVID-19 is likely to last for years to come. These resources are critical and necessary to ensure that all citizens who need benefits can successfully interact with state governments in a timely and secure manner. It is for these reasons that we request federal funding for our state IT agencies in order to continue to appropriately respond to the COVID-19 pandemic and to address the increasing cybersecurity risks to state systems.

As Congress considers additional legislation related to COVID-19 response, we encourage you to:

- **Authorize and appropriate dedicated cybersecurity funding for state governments**
  Throughout the 116th Congress, bicameral and bipartisan cybersecurity legislation for state and local governments has been focused on the modernization and security of IT systems in order to better protect citizen data, improve digital service delivery and ensure that state and local governments are able to effectively and capably adjust to changing dynamics as a result of COVID-19. IT agencies continue to defend state systems from a constant barrage of coordinated and sophisticated cyber attacks, but funding to allow for the investment in training for state employees, multifactor authentication, endpoint security, software patching tools and remote security assessments, among many other high priority items is needed across the country.

- **Allow for the flexible utilization of this funding to help states address both cybersecurity and IT needs associated with increased use of state networks in response to COVID-19**
  For nearly the past decade cybersecurity and risk management has been the top priority for the nation's CIOs. While we do not expect this focus on security to change, the ongoing pandemic has exacerbated significant issues with legacy systems and platforms across state networks. Any funding provided to state governments through additional legislation should allow IT agencies latitude and broad flexibility to direct resources to their states' most critical technological needs.

- **Include S. 2749, the *DotGov Act* to ensure local governments are better equipped to combat widespread misinformation and disinformation surrounding COVID-19**
  NASCIO has been a longtime advocate and supporter of the adoption of the DotGov domain for state and local governments, primarily due to its security functions. However, nearly twenty years after making DotGov available to state and local governments, the vast majority of local governments are still not making use of this advantage. As of today, there are only approximately 8.5 percent of all eligible local governments on the DotGov domain. As citizens seek information concerning the pandemic from government websites in unprecedented numbers, we have seen a significant increase in misinformation, spoofing and conspiracy theories about COVID-19. Inclusion of the bipartisan *DotGov Act* would provide a low-cost tool for local governments to ensure the authenticity and security of their websites.

On behalf of the nation's state CIOs, we greatly appreciate your consideration of these requests and appreciate your bipartisan efforts during this unprecedented moment in American history. Should you have any questions, please contact Matt Pincus, NASCIO Director of Government Affairs, at mpincus@nascio.org or 202.624.8477.

Sincerely,

Denis Goulet
NASCIO President and New Hampshire CIO

Doug Robinson
NASCIO Executive Director