State IT Update: COVID-19 Response and Recovery

NCSL Cybersecurity Task Force Meeting
April 28, 2020

Doug Robinson
Executive Director, NASCIO
STATE CIO TOP 10 PRIORITIES
2020 Strategies, Policy Issues and Management Processes

1. Cybersecurity and Risk Management
   #1 for seven consecutive years. On the top ten list since 2006

2. Digital Government
   Steadily moving up the list. #4 in 2019

3. Cloud Services
   Major force of change

4. Consolidation/Optimization
   CIO priority each year. On the top ten list since 2006

5. Customer Relationship Management
   A key issue because of business model. On the list since 2009

6. Budget, Cost Control, Fiscal Management

7. Legacy modernization

8. Data Management and Analytics
   Holding steady on the list since 2016

9. Broadband/Wireless Connectivity

10. Innovation and Transformation through Technology
    First time on the top ten

NASCIO
Representing Chief Information Officers of the States
STATE CIO TOP 10 PRIORITIES
2020 Strategies, Policy Issues and Management Processes

1. Cybersecurity and Risk Management
   #1 for seven consecutive years. On the top ten list since 2006

2. Digital Government
   Steadily moving up the list. #4 in 2019

3. Cloud Services
   Major force of change

4. Consolidation/Optimization
   CIO priority each year. On the top ten list since 2006

5. Customer Relationship Management
   A key issue because of business model. On the list since 2009

6. Budget, Cost Control, Fiscal Management

7. Legacy modernization
   Holding steady on the list since 2016

8. Data Management and Analytics

9. Broadband/Wireless Connectivity

10. Innovation and Transformation through Technology
    First time on the top ten
COVID-19 Response and Recovery

Secure remote access; remote workstation deployment

IT infrastructure/systems stability, scaling, configuration

Cybersecurity and risk management

Teleconference/video conferencing/call centers

Corporate partners and the IT supply chain

COVID-19 recovery phase and the Big Return?
<table>
<thead>
<tr>
<th>State Cyber Issues to Watch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support and assistance to local governments</td>
</tr>
<tr>
<td>Elections security and disinformation</td>
</tr>
<tr>
<td>Risk of emerging technologies – AI, IoT, UAS</td>
</tr>
<tr>
<td>Third-party contractor security risks - outsourcing</td>
</tr>
<tr>
<td>IT supply chain risks</td>
</tr>
<tr>
<td>Public records laws/FOIA exemptions for cyber</td>
</tr>
</tbody>
</table>
Action is Needed Now

1) At the very minimum states should be building relationships with local governments.
   - Work through state municipal leagues and county associations, with emphasis on local information technology associations.

2) States should raise awareness of existing services being offered to local governments.
   - Hold cyber summits
   - Educate stakeholders

3) States should be exploring cost savings that can be achieved through including local governments in service contracts.
   - Consult local governments during the contract planning process solicitation
   - Provide a conduit for discussions about pooling resources among shared risk pools at the local level