NASCIO
Representing Chief Information Officers of the States

COVID-19 Planning and Response Guidance for State CIOs

Version 2.0

(March 26, 2020)

Today we are facing the COVID-19 (novel coronavirus) global pandemic. All states have a COVID-19 outbreak and the situation is dynamic, expanding and moving fast. As the business leader of state information technology (IT), state chief information officers (CIOs) play a critical role in the response to and recovery from this public health emergency. During a time of mandatory remote work and shelter in place, IT is playing a vital part in the continuity of state government. Critical questions for state government include the following.

- What is the role of the state CIO in coordinating a response with the governor's office and other state agencies?
- What is the role of the state CIO when planning for reduced staff?
- What are the critical issues that need to be prioritized to ensure continuity of IT operations for your state?
- What are challenges related to expanded remote access for employees?
- What are the actual and potential cybersecurity risks?
- How does the current circumstance impact the current project portfolio?

State CIOs have an obligation to ensure that IT services continue during this pandemic outbreak and planning for such a scenario has become essential. ***As such is it imperative that state CIOs have a seat at the table with government leaders and take an active role in the state response to COVID-19.*** There are critical steps that state CIOs can follow during the next days and weeks.

COVID-19 Planning 101

The primary focus of this brief is how to maintain critical operations and services during the COVID-19 pandemic outbreak. The learnings gained from this current circumstance will begin to build the necessary wisdom for dealing with future pandemics. Pandemics are unique in that they primarily affect an organization's workforce as opposed to its physical infrastructure, and therefore require a radically different approach for recovery efforts. Planning in response to a pandemic event should include an incident management component involving an incident command response and identifying those key members and players necessary for a comprehensive solution to the plans that are developed.

The impact of a pandemic on the state IT organization goes beyond just the people, process and technology aspects. On a larger scale, with the new operating model of the state CIO as a broker of services rather than a provider of services, the CIO must understand the impact to the logistics of contractors and suppliers outside of the state IT organization who may also be experiencing a high rate of employee absenteeism, and potentially greater demand for their services. CIOs must determine how to communicate a lapse in service to agencies when it is out of their control.

Public health experts agree that COVID-19 will continue to spread over the next several weeks or months and will result in a high rate of state employee absenteeism, disruption of commerce, supply chain issues and constrained access to critical resources. Most states' IT organizations are simply not prepared to address the infrastructure and procedural issues that will emerge as a result.

State IT leaders need to make sure their disaster recovery / business continuity (DR/BC) plans are designed to deal with this type of contingency. Consciousness is being raised on several fronts, and state IT – for the most part – has started taking the necessary steps to implement and test plans and processes to cope with this type of outbreak.

These circumstances include the added challenges related to increased demand for certain government services related to the emergency response. State governments are already experiencing another dangerous element. Cyber criminals and nation states are taking advantage of these circumstances and counting on state governments to be less vigilant regarding cyber-attacks and potential cyber disruptions. States must increase their vigilance regarding both types of events. Cyber-attacks and the more ominous and longer duration cyber disruptions.

The Role of the CIO in COVID-19 Preparedness and Response

When systems are down and every aspect of state business is affected, the buck may stop at the CIO's desk. However, there are critical steps that CIOs can follow to ensure that their IT infrastructure is protected under any scenario. One major difference in a pandemic crisis versus an unforeseen disaster is that there is an element of nature that may provide the luxury of time. There is typically a gradual escalation of such events as they emerge as an epidemic or pandemic. The CIO can start to respond and escalate a response but identifying the critical triggers and executing successfully on those must be in the state's overall DR/BC plan. There should be predefined stage gates and clear decisions regarding escalation of the CIO's response plan. However, as events unfold, there is a degree of uncertainty regarding the magnitude of how such an event may persist. CIOs need to identify critical staff and business functions that their state enterprises cannot function without. The critical business functions and critical staff tiering for a pandemic may be completely different from that for a physical disaster. Unlike other DR/BC situations, in the case of a pandemic, the critical staff list should include for example, those operating the data center's general maintenance functions as well as those in charge of cybersecurity. Finally, prepare for making decisions in an environment of uncertainty. ***During a crisis the CIO may not have all the information necessary but will be required to make immediate decisions.***

Planning and Preparedness

Update your DR/BC plan to address the unique problems associated with a pandemic event—This plan should include:

(1) A focus on capabilities that are needed in any crisis

(2) Identification of functional requirements

(3) Planning based on the different severity levels of a pandemic event

(4) Service level requirements for business continuity

(5) Revisions and updates—having critical partners review the plan

(6) Storing hard and digital copies of the plan in several locations for security

Pandemic preparedness coordinating committees – Gather representatives from all applicable lines of business and critical services necessary for continuity of IT operations. Keep the dialogue open with state business partners and periodically convene briefings for them on the state's DR/BC plans.

Ask and answer the following questions— (1) What are the top business functions and essential services of the state enterprise? Develop a common and consistent definition of "essential services." Tier business functions and essential services into recovery categories based on level of importance and allowable downtime. (2) How can disruption to an agency's or department's operations be reduced?

Conduct contingency planning in case of absent personnel – This could involve cross-training of essential personnel who can be lent out to other agencies in case of loss of service. Also, mutual aid agreements with other public/private entities such as state universities for "skilled volunteers" can be put in place. Make sure contractors and volunteers have approved access to facilities during a crisis.

Approach enterprise backup as a shared service - Other agencies may have the capability for excess redundancy.

Review and suggest revisions to state personnel policies that offer flexibility – During a pandemic crisis, state IT employees may be asked to work under conditions not traditionally covered under current state policy. State CIOs should meet with state personnel officials, employee unions and associations to discuss flexible policies that can be temporarily implemented during a pandemic crisis. In this manner, decisions made by the CIO concerning who stays on site, who goes home, and issues about pay, leave, and state liabilities can be adequately addressed. Review statues and policies on holding official meetings virtually.

Review state and federal regulatory requirements regarding business processes and IT service levels– During a pandemic crisis, state IT organizations may find that mandatory service delivery associated with state and federal programs is temporarily disrupted and service level agreements are not being met. Federal programmatic funding may require certain service performance levels that cannot be met during a pandemic. In such a situation, the CIO may need to seek waivers from the federal government, or temporarily seek service freezes because of IT operational concerns. Investigate the process and options before seeking relief ahead of the crisis!

Manage customer relationships—This is an important time to focus on customer relationship management. Most state agencies are unable to deliver normal business functions and sustain operations. Customer behavior and response may be difficult because they are under significant stress and uncertainty. State CIOs need to have conversations with agency business partners about disruption to manage expectations and answer questions about rates and service level agreement provisions.

Build on internal relationships with emergency, health and homeland security officials – CIOs should continue to build upon existing relationships with state-wide agency and local emergency management and health department personnel and other necessary stakeholders. A CIO should know and communicate with his or her emergency management counterparts before and during crisis.

Prepare for limited or zero access to your facilities – Even though IT personnel may be theoretically available during a crisis, the structural environment in which IT systems are located may be where a pandemic exposure level is rising. If the area is quarantined and access is prohibited, there exists a serious problem. CIOs must look at how they would manage the situation as it is beginning to build. If a facility becomes contaminated or is in a quarantine zone, state health officials are probably not going to allow access. It may be possible to seal the area off and gain approval for controlled access of critical personnel. (Thus, be sure to coordinate with state health departments in advance. Make them aware that they may not be able to access critical health files if the state's primary computing facilities are non-operational.)

Prepare to treat state IT facilities as disaster areas and go into full DR/BC mode—If access is denied to critical state data facilities and the result is a failure from the technology side, the state CIO must be prepared to enter into full DR/BC mode. Due to a potential lack of access, a CIO may be in the position to declare a full-scale disaster. In addition, the CIO should prepare to conduct business off-premise. Today's cloud-based DR/BC services are capable of meeting this demand, however, be prepared for slower than normal response as other public and private sector organizations are competing for the same resources.

Communication

Activate your media crisis communications plan and protocol—A crisis communications protocol should be part of a state's IT DR/BC plan. Designate a primary media spokesperson with additional, single point-of-contact communications officers as back-ups. Articulate who can speak to whom under different conditions, as well as who should not speak with the press.

Anticipate the need for a robust livestreaming capability for governors and key state officials– Citizens and the media expect regular, live updates on the status of the pandemic. These events must be livestreamed to a variety of end user devices and the delivery platforms must scale well beyond a typical audience. With social distancing or isolation in effect, governors may need to conduct press briefings via remote locations with high quality streaming video.

Educate state IT staff on basic preparedness for themselves and their families –Work with state public health agencies for basic information and build a packet tailored to state IT staff.

Educate state IT staff, lawmakers, appointed officials, human resources and budget officials – Craft an education and awareness program for state IT staff, lawmakers and budget officials to ensure all parties are on the same page with regards to the pandemic preparedness plan and the need for such a plan.

Communication and cross-boundary collaboration – Make sure state workers are trained on remote access technology. Utilize critical partnerships with other agencies and branches of government. Think outside the box: CIOs can partner with anyone to share IT resources; including universities, local government, lottery corporations, local companies and leased facilities with redundant capabilities.

Classify and cross-train IT employees –In most other events, the CIO can designate who responds. Yet, with pandemics, the CIO has no control over who is sick. Decide now which employees can function in multiple roles and think about cross-training critical roles now. Consider having critical employees work in shifts if they must come into the office.

Intergovernmental communications and coordination plan – Develop a plan to communicate and coordinate efforts with state, local and federal government officials. Make sure jurisdictional authority is clearly established and articulated to avoid internal conflicts during a crisis.

Communicate to rank and file employees—Explain there is a pandemic plan and the reasons behind its establishment. Clearly articulate employee roles during a pandemic incident and identify members of a possible crisis management team.

Technology Infrastructure and Services

Remote work – The tactical use of telecommuting for critical personnel may resolve many on-site accessibility problems and is the major topic of discussion today regarding the impact of COVID-19. Working remotely is easier than ever today with widespread state-issued laptop deployment, tablets, smart phones and apps that make work easier. Anticipate and be prepared to address the following:

- Broader distribution of guidance and educational materials for remote workers. State websites with detailed instructions on computer configuration and use are a necessity.
- Requests for relaxation or suspension of standard security policies and protocols. With a significant remote work force, temporary changes to the password expiration policy may be necessary.
- High demand for state-issued laptops, tablets and smart phones.

- Being flexible with technology deployment for remote work. State employees without a laptop computer may need to bring their desktops and monitors home. Additional helpdesk support might be required to assist them in setup and configuration.
- Expanded use of remote access tools, collaboration and enterprise instant messaging platforms, including web video conferencing. Given typical use in state government, this will require adjustment to end user concurrent licenses.
- Expansion of virtual private network (VPN) access and licenses.
- Expansion and use of virtual desktop infrastructure (VDI) to provide access to employee desktops back at state office.
- Most states prohibit the use of home computers and personal technology devices (BYOD) by state employees to access state systems. From a support and cybersecurity standpoint, using home computers and personal devices is strongly discouraged. If this is necessary and permitted by an exception policy, ensure all security controls are configured and updated. VDI is another option that states are deploying for using use home computers.

Distribution or redeployment of state-issued laptops, keyboards, mice, tablets, smart phones, printers or accessories should include one additional step – a physical disinfection process. Like similar viruses, studies suggest that COVID-19 may persist on surfaces for a few hours or up to several days.

Around 75% of US adults have broadband internet service at home according to Pew. With these technologies, working from home has become much more mainstream and accepted in workplaces than it was a decade ago. However, with bandwidth-intensive applications such as collaboration platforms and video conferencing, plan for diminished quality of service and possible interruptions. With the COVID-19 pandemic to date, large organizations such as state governments have been experiencing intermittent service disruptions because of overwhelming demand.

Provide remote workers with guidelines for working at home including steps to access technology as well as expectations. Understand that work may need to take place outside of normal business hours if employees are caring for sick family members or have been left without childcare. Provide flexibility outside of normal policies to account for this.

Identify essential critical infrastructure workers for telecommunications and IT—During a widespread pandemic with restricted access to government facilities and disruption to work schedules, state CIOs will need identify essential IT employees required to maintain the continuity of government operations. Classes of these employees may include data center operators, system administrators, telecommunications technicians, cybersecurity professionals and help desk support. Some of these employees may be working remotely to support the mission of state agencies. DHS CISA has developed, in collaboration with other federal agencies, state and local governments, and the private sector, an "Essential Critical Infrastructure Workforce" advisory list. This list is intended to help state, local, tribal and territorial officials as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security.

Assess, prioritize and shutdown non-essential services – This will free up resources for other critical services. Identify critical business applications and essential services and then tier them into recovery categories based on level of importance and allowable down-time. Understand that applications may be overwhelmed—such as unemployment assistance—and prioritize those. Helpdesks may be overwhelmed due to absenteeism and a higher number of workers needing help with remote technologies. Consider utilizing chat services or bots where it is sensible to do so.

Voice telecommunications – With widespread adoption of cloud-based voice over internet protocol (VoIP) systems, state governments now have more scalability and flexibility to deploy softphone options. CIOs will need to determine the features and differences between the current tiers of services and an expanded end user base. These systems have a host of advanced features and capabilities that are probably unknown to most of the state government workforce. State workers have little experience working remotely with advanced configurations and call forwarding to smart phones. Pre-configuration, guidance and end user training will be required.

Reexamine change control schedule and system updates – With a pandemic underway, a seven-day work week may be required for some time. Standard weekend schedules for system and software updates should be adjusted as needed or deferred to avoid business disruption.

Leverage existing technology platforms and services – During a pandemic event, geographic information systems (GIS) platform(s) should be utilized to monitor COVID-19 tracking and provide dashboards of the outbreak. Data visualization tools are very effective in delivering complex data and real time situational awareness for both internal and external users. For broad communication and notification to citizens, a COVID-19 website is an imperative. To provide easy and intuitive access, the state's homepage should provide direct access or be temporarily converted to a pandemic communication portal.

Expanded Helpdesk Capability—With more IT and other state employees using remote technologies for the first time, there will be a higher need for helpdesk support. Staff augmentation through contractor services may be required. Consider implementing cloud-based helpdesk services, chat services and bots as appropriate. CIOs may need to expand current off-premise provider services and scale up quickly to meet demand.

Utilize the National Guard for Emergency Support Function (ESF) 17 – In response to COVID-19, several states have activated the National Guard. If needed and available, the National Guard can provide supplemental cybersecurity resources to the state CIO organization during the emergency.

Cybersecurity Risks

Balance cybersecurity risks with business continuity – State CIOs and chief information security officers (CISOs) should plan for increased vulnerabilities while continuing to support the needs of state agencies to conduct business. Cybersecurity risks both from hackers looking to take advantage of the situation and play off people's fears (such as recent phishing scams related to COVID-19) and additional vulnerabilities from a higher number of workers using VPN and home networks to work remotely.

- Expect cybersecurity threat campaigns targeting states and COVID-19 related opportunistic attacks
- Ensure VPNs and remote access systems are fully patched

- Enable or expand multi-factor authentication
- Enhance system monitoring to receive early detection and alerts. Before sending state employees home with laptops, make sure they have properly configured firewalls as well as intrusion prevention and anti-malware software installed. The document CISA Insights: Risk Management for Novel Coronavirus (COVID-19) is a good resource.
- Proactively monitor remote access users for excessive use of non-business-related websites and unacceptable behavior that may place the state at risk. Employees are under significant stress and may not be making wise choices.
- Review state plans to deal with a cyber disruption to ensure the plans are up to date and the necessary governance, relationships, emergency support functions (ESFs) and critical staff roles are in a strong position of readiness.

Cybersecurity risks due to absenteeism--Prepare for problems arising from absent cybersecurity staff due to illness. CIOs should also consider the risk of a cybersecurity incident due to absenteeism on the part of a cybersecurity contractor or managed services provider. Discuss these challenges with your suppliers and contractors and stay up to date on their status.

Securing Online Video Meetings—As more schools, businesses and individuals have moved to online video conferencing, there have been reports of individuals dropping in on meetings or classes and sharing inappropriate content (known as "Zoom-bombing"). Users should take steps to securing these meetings using passwords, the waiting room function, and not sharing links to meetings in public platforms. More information and tips can be found from the FBI.

The Supply Chain

Consider outside entities that provide supplies and support – Consider critical support elements such as contractors, vendors and sites that they provide and the consequences of disruptions in those services. CIOs also need to examine services that provide basic necessities, such as the power grid that supplies power to state IT facilities.

Handling package shipments to the CIO organization – According to the USPS, packages are relatively low-risk for transmitting the novel coronavirus. Current guidance is to wait 24 hours before handling cardboard. However, disinfecting the shipping boxes with a quick disinfecting wipe is advisable as a precautionary measure.

Review state contracting instruments and laws – Set up emergency standby services and hardware contracts and have contracts in place for products and services that may be needed in the event of a declared pandemic emergency. Create a contract template so that a contract can be developed with just one or two hours work time. CIOs must be sure essential IT procurement staff are part of the DR/BC plan and are aware of their roles in executing pre-positioned contracts in the event of a disaster. CIOs should also develop "Emergency Purchasing Guidelines" for agencies and have emergency response legislation in place.

Enterprise Portfolio Management and the Service Management Catalog

Evaluate the impact on the current project portfolio – Some projects will have to be adjusted to have a longer duration or a work stoppage. This can be a result of the diverting workforce to other tasks related to the current emergency, the unavailability of agency staff, or the delays associated with reorganizing the project and the project team.

Evaluate the impact on service availability - Services that are being delivered or contracted may be affected depending on the nature of the emergency. Assess the service catalog for potential impact on service level commitments. Some government services will be in higher demand or even significantly higher demand depending on the emergency. The increase in the demand for these services will inherently put more demand on certain technology resources such as network bandwidth. The nature of the emergency may also require a faster response rate on service delivery – i.e., more service capacity and faster service capability.

Cross Boundary Collaboration and Relationships

Like many disasters, pandemics are not constrained by state borders and geography. Consider reaching out to your state CIO counterparts in the region to share information and partner on solutions. Some states already have cross boundary DR/BC agreements and others have arrangements with major universities. Local government CIOs may need your assistance or have valuable response information to share. Be creative and seek all opportunities to collaborate.

Final Considerations: What's Next?

State CIOs, as much as possible, should not focus on the geo-political aspects of a pandemic incident, but instead focus on "how does this directly affect my IT enterprise operations?" and take immediate steps to keep the state's essential IT business functions operating. CIOs should rely on federal, state and local emergency management and health officials to handle the wider "big picture" issues of disrupted commerce, the general health and well-being of the populace, and potential control and protection of a panicked populace.

This is the time to promote and expand the advantages of enterprise platforms, software-as-a-service, cloud services and cybersecurity services. These environments are more adaptable and can scale quickly if needed. With most states already consolidating IT infrastructure, data centers with secondary back up or utilizing cloud services, taking these additional steps may not be thinking too far outside the box. Challenges remain for the foreseeable future, but state CIOs are uniquely positioned to help their states get through this pandemic.