# Harnessing Visibility and Analytics to Lead Citizens Through Change

## The New Tomorrow for State and Local Government

Gigamon®

# Executive Summary

The world changed suddenly for state and local governments. In a short period, COVID-19 and its aftermath forced a transformation in how states and municipalities deliver services to citizens. With little time to prepare, state and local governments were thrust into leadership roles in the public health crisis response. Meanwhile, the need for reliable access to government services escalated to unprecedented levels.

Pressure on web-based platforms exploded overnight. State unemployment systems were pushed far beyond their limits. Government sessions, public meetings and education shifted to online meeting platforms. These and other forced technology shifts generated a wave of unplanned IT demands and technical support challenges. Meanwhile, growing crisis response costs, skyrocketing unemployment and lower tax revenue created severe budget pressures at the state and local levels of government.

State and local governments were already facing significant challenges before COVID-19. However, the crisis is an inflection point for many. The need for resilience and agility as pressure mounts from every direction is leading many elected officials and government employees to rethink how technology can transform the way that government works. This reimagining of government is likely to continue even after the current crisis is behind us.

# Overview

This paper explores IT priorities that state and local governments will need to address today, in the Return-to-work transition and in The New Tomorrow.

## TODAY

The imperative is to continue delivering critical services to citizens while ensuring the continuity of government. This includes providing operational support to agencies with widely varying charters and needs. In most cases, this must be achieved while working under suboptimal conditions and with reduced budgets and resources.

## RETURN TO WORK

State and local governments were forced to close facilities and transition to a work-from-home model (WFH) in a matter of days and with minimal planning. However, the Return-to-work process will take significantly longer, and the nature and timing of this process are still uncertain.

## THE NEW TOMORROW

Faced with uncertainty, challenges and opportunities, state and local governments must develop constituent services and governing models that cover a number of possible futures and build an agile network and security infrastructure to support these models.

We would like to share our thoughts on how state and local governments can best navigate these challenges and opportunities and equip their NetOps and InfoSec teams to be successful in these unprecedented times.

# Today

As the immediate impact of the COVID-19 crisis has stabilized, state and local government IT teams now face a new set of challenges driven by four key imperatives.

## Deliver Constituent Services Online

Delivering the services that citizens depend on is an essential mandate for state and local governments. Many states and municipalities have transitioned to online models for many services. However, less-critical functions that were temporarily paused or scaled back must also be incorporated into an online model or revisited with a more systematic in-person approach.

In addition, systems that buckled under the added pressure that the COVID-19 crisis placed on them must be rebuilt for scale and resilience. State unemployment claim processing systems are a notable example. As tens of millions of claims were submitted over several weeks at the height of the crisis, citizens in dire need of assistance faced days of frustrating errors and uncertainty as IT teams scrambled to scale up antiquated systems built with legacy programming languages like COBOL.

Emerging technology implementations that are still in their infancy must also be scaled and matured quickly. For example, many local transit systems are in the early stages of offering electronic, contactless fare collection. Prior to COVID-19, these services were utilized by a small subset of riders. However, the need for social distancing requires operational changes such as all-door boarding and limiting staff contact with riders, making electronic fare collection the default option instead of a choice for early adopters.

In addition, providing high-quality, technology-enabled services to citizens often means redeploying existing applications to new, more scalable cloud-based architectures or bringing new SaaS-based applications online. As these new applications, microservices and virtual machines are deployed, IT and infrastructure teams risk being left behind by fast-working DevOps and applications teams and outside consultants who may disengage once the crisis is over. This can have serious consequences unless these teams work closely together.

## Accomplish More with Constrained Budgets

As of June 2020, half of all state governments had made supplemental budget appropriations or tapped rainy day funds to support COVID-19 response efforts. The impact of these unplanned budget moves is being compounded by other factors such as reductions and delays in tax payments and increased unemployment insurance costs. California alone faces a $54 billion budget shortfall. Meanwhile, local governments are already beginning employee furloughs and layoffs, including for first responders and other critical personnel.

From an IT perspective, the pressure to accomplish more with less has never been greater. It is critical for security and network teams to find ways to work more efficiently and extend the life of their existing tools and infrastructure.

## Optimize the Work-from-Home Model

For most state and local government entities, the shift to a WFH model left IT teams with little time to plan or scale their remote access infrastructure. However, most states and municipalities have stabilized their WFH capability now and are focused on optimizing this environment to provide the best possible user experience to their employees.

This WFH capability is often dependent upon video conferencing applications such as Zoom, WebEx and Microsoft Teams. While these apps are SaaS-based and can scale rapidly, they can also place a heavy load on network bandwidth, resulting in a poor user experience. Additionally, well-publicized security weaknesses in some of these apps and the non-standard ways that departments and individuals use these apps may pose potentially serious security issues.

## Secure the Network

Bad actors quickly exploited the disruption caused by COVID-19 to compromise newly expanded network infrastructure, applications and users who had not been fully trained in remote working procedures and security awareness.

Even after a wave of high-profile phishing and ransomware attacks crippled many state and local governments in 2019, few had time to shore up their defenses prior to the COVID-19 crisis. In a January 2020 poll by Harris and IBM, half of the state and local government employees surveyed had not seen any changes in preparedness by their employers. Only 38 percent had received training on ransomware.

More online interaction between government entities and community members only increases the number of attack vectors as bad actors pivot their tactics to exploit the crisis.

More online interaction between government entities and community members only increases the number of attack vectors as bad actors pivot their tactics to exploit the crisis.

# Return to Work

Today, almost all state and local government entities are focused on the questions of when they can return to work, what the new model will look like and whether there will be a second wave of COVID-19 infections to contend with. As stay-at-home orders are gradually relaxed, many states and municipalities are bracing for additional periods of disruption. This requires a careful balancing act of restoring traditional in-person functions while also continuing to invest in technologies that support remote work and online government services.

## Transition Employees Back to Government Facilities

State and local governments in the U.S. employ over 17 million people, so transitioning all employees back to on-site work will be a substantial undertaking. It will likely require a phased approach, and IT teams must be prepared for unexpected spikes in infrastructure usage as waves of employees shift back to government facilities. In addition, some employees and departments may continue WFH and online service delivery models indefinitely, so remote access and online infrastructure investments may need to continue in parallel for the foreseeable future.

In a world where many government employees need to operate on an "access anywhere, anytime" remote work model, moving to a Zero Trust architecture not only makes sense, it is close to an imperative.

## Enhance Network Visibility and Performance

Faced with the combined pressures of supporting on-site workers, remote workers and community members accessing services online, IT teams will require added visibility into infrastructure performance and tools at their disposal to diagnose and correct issues quickly. This is particularly critical for government agencies that were forced to pause or scale back services during the crisis and now face a backlog of demand. In both direct engagement and self-service interactions, harnessing technology to restore public confidence will be essential.

In addition to bolstering critical IT resources, IT teams must also find ways to tune out noise that can overwhelm both tools and personnel. For example, as the use of Zoom and other video conferencing services rises, the impact on network infrastructure and monitoring tools is significant. IT teams must find ways to filter high-volume traffic that poses a low level of risk to reduce the burden on network infrastructure and tools.

## Embrace Partnerships with the Private Sector

One notable technology success story to emerge from the COVID-19 crisis is the rapid development of public-private partnerships in the area of contact tracing. Many states, as well as large municipalities like New York City, have partnered with technology vendors like Salesforce to enable large-scale contact-tracking infrastructure in the cloud. Similarly, Apple and Google forged a collaboration to provide contact-tracing functionality in their mobile operating systems that can be leveraged by state-managed contact-tracking applications.

These types of partnerships, born out of necessity during a crisis, can serve as a blueprint for innovative use of the cloud, mobile devices and other innovative technologies under non-crisis conditions in the future.

## Reevaluate Security

Now is the right time for state and local government InfoSec and SecOps teams to reassess their security models, procedures and tools. However, for many states and municipalities, the reality is that they went into this crisis with significant security vulnerabilities as a result of:

+ Understaffed InfoSec and SecOps teams
+ Undertrained end users
+ Vulnerabilities arising from outdated computer systems and IT infrastructure
+ Massive growth in traffic as a result of remote work
+ Spikes in demand on antiquated systems for unemployment claim processing and other key government services

These issues have now been compounded by the additional stress that the crisis has placed on security staff, tools and budgets. While the correct security approach will vary based on each state or municipality's unique situation and resources, the key building blocks for a successful, agile security model are ensuring end-to-end visibility into all network traffic; AI- and machine learning-based analytic tools that detect and prioritize anomalies and threats; and automation tools that handle mundane tasks and free security teams to focus on the highest priority issues.

For some states and municipalities, this security review may include consideration of a Zero Trust model. In a world where many government employees need to operate on an "access anywhere, anytime" remote work model, moving to a Zero Trust architecture not only makes sense, it is close to an imperative. Because the network is under constant attack from a huge array of external and internal threats, all users, devices, applications and resources must be treated as being hostile. These users and devices need to be rigorously authenticated, and data and other network assets need to be protected at a much more granular level than perimeter-based security models allow.

# The New Tomorrow

Many forward-thinking state and local governments are already looking beyond today's crisis recovery situation and reimagining the way they serve the public in what people are calling the New Normal, the Next Normal or The New Tomorrow.

As in any period of economic turmoil, The New Tomorrow will bring new challenges and opportunities. While the degree of change, challenge and opportunity will vary based on the resources and risk-tolerance of individual states and municipalities, those that thrive in The New Tomorrow will share a number of characteristics in their cultures, operational models and supporting infrastructures. These governing bodies will be resilient, innovative and forward-looking. They will develop governing and operational models that can respond quickly to changing community needs, and they will have IT infrastructures that mirror these core values.

### ✓ VISIBILITY

You can't manage what you can't see, and gaining visibility into all network traffic will become a survival issue for many state and local governments. The physical, virtual and cloud-based visibility into both encrypted and unencrypted data that Gigamon provides is already trusted by many of the world's most demanding organizations, including many government agencies and private sector businesses.

### ✓ AGILITY

As recent events have shown, agility doesn't just mean handling the pressures of growth and innovation; it also means handling unforeseen and unprecedented change. In this situation, it is critical that state and local government networks and security capabilities support continued changes in working practices and community infrastructure usage, and new tools deployment. In addition, building on the private sector partnerships forged during the COVID-19 crisis will help state and local governments increase their agility by applying innovations from commercial organizations to public sector IT challenges more rapidly.

### ✓ COST OPTIMIZATION

The effects of COVID-19 on state and local government budgets will be felt for years to come. However, this should not prevent government IT teams from pursuing innovation. Even as budgets remain uncertain, state and municipal IT teams have opportunities to unlock additional value from their existing IT investments. Granular visibility into how network infrastructure is used and intelligent use of data filtering to focus network and security tools on the most relevant activity will help government IT and security teams focus on higher-value activities while controlling costs.

### ✓ CLOUD

For both time-to-market and scalability reasons, the cloud is the preferred application deployment platform for The New Tomorrow, whether in the form of SaaS-based apps or custom applications that reflect an agency or locality's unique needs and capabilities. As cloud adoption accelerates, maintaining visibility into all information — regardless of whether it is on-premises or in the cloud — and having the ability to secure it, becomes an increasingly important mandate for successful states and municipalities.

# Final Thoughts

The COVID-19 crisis has set off a chain reaction of events that will profoundly affect our society and economy for the foreseeable future. Leadership and innovation at the state and local government levels can play a transformative role in the everyday lives of citizens. In the short term, delivering essential government services as effectively as possible is a critical priority. However, many opportunities exist to apply the lessons learned from this crisis to improve how governments serve their citizens, as well as mitigate the impact of future crises. Meeting immediate needs while also taking full advantage of the opportunities that lie ahead will require resilience, agility and visibility in every aspect of governmental operations, including networks and information security systems.

# About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual and cloud networks to solve critical security, performance and business continuity needs. The Gigamon Visibility and Analytics Fabric$^{TM}$ delivers optimized network and security performance, simplified management and accelerated troubleshooting while increasing your tools' return on investment. Our comprehensive solutions accelerate your organizations' ability to detect and respond to security threats including those hidden in encrypted traffic. Trusted by 83 percent of the Fortune 100 and 4,000 organizations worldwide, Gigamon ensures that your business can run fast and stay secure in The New Tomorrow.

**For the full story on how Gigamon can help you, please visit gigamon.com.**

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com