Defining Mobile Strategy for Government

How state and local agencies can build mobility into productivity

CITRIX® Public Sector

What Does Mobility Really Mean for Government?

Defining a mobile strategy that is designed for state and local

Mobility can mean a lot of things to different people. Most think about the device that's in their hands or pocket — maybe it's the ability to connect online via a tablet or laptop — and the generic term usually describes a person's ability to untether from the office. But, mobility is much more than just a device or concept. Mobility is a strategy that technology leaders can use to redefine access, control and security, says David Smith, the Director of State and Local Government for Citrix.

"When I think of mobility, I like to ask myself, regardless of where I am — Can I get to that critical application or data to do my job?" Smith says. "If the answer is 'yes,' and I'm able to do so in a way that's highly secure and optimized for the situation that I am in, then that's mobility."

For government, mobility means being able to work and be productive from wherever you are. Increasingly, state and local government employees are moving out from behind the desk and making mobility a job requirement . Agencies that optimize to meet mobility needs can often times cut costs, improve efficiencies and even transform the workplace culture overall.

The U.S. workforce at large is more mobile than ever before. Recent trends indicate that employees operate outside of the routine 9-to-5 period, and most are working from remote access points, which require access. In fact, 45 percent of the U.S. workforce holds a job that is compatible with at least part-time telework. The vast majority of those members — 76 percent of work-at-home employees — work within the private sector, but there's a growing number of state and local employees joining the ranks as well.

Today, 40 percent of state and local government employees are using mobile devices and 17 percent are eligible to telework. Some states, including Georgia, Virginia, and Arizona, have passed legislation to increase work-at-home access within their state agencies. But, most states have yet to fully implement a mobile strategy.

Still, more than half — 58 percent of state employees — say their agency is not mobile

ready, and most do not adequately provide the plans, tools and support necessary to manage a mobile workforce.

Mobile-ready agencies **gain three additional hours of productivity**, per employee, per week.

Citrix "State & Local Mobility Map: Road to Mobile Readiness" Survey

"With a mobile strategy, government IT departments can acquire, provision and support devices with integrated connectivity," Smith says. "This approach to mobility also helps the organization focus on three key things: access, control and security."

Access is the first step to ensure that mobility is designed to meet the changing needs of the government workforce. As workplace mobility increases, so too must control. Many workers are now using personal devices, such as smartphones, to support their productivity. This often is a conscious choice to use the same device for both personal and business work functions, referred to as "bring your own device" (BYOD). Allowing users to bring their own devices to work is gaining in popularity, especially as BYOD policies begin to address security concerns.

"We can look at mobility in two ways," Smith says. "Mobility is a device challenge, and it's a security challenge too. A lot of change is happening in the technology space. New devices are always available, but so is more risk. From a security standpoint, there's a greater chance to expose sensitive data, particularly citizen data."

Allowing users to bring their own device to work does bring with it some inherent security challenges. 75 percent of mobile security breaches are the result of mobile application misconfiguration, according to a Gartner survey. Other risks

8 Steps to Making Mobile Work

Take these eight steps to provide greater access, control and security

1. Enable mobility for workers, applications and data
2. Keep highly sensitive data in the datacenter whenever possible
3. Protect distributed mobile data in an encrypted secure container
4. Enforce policies specifying what should happen under specific contextual circumstances
5. Control data distribution and usage through policy
6. Personalize the worker experience for optimal productivity
7. Automate both the desired worker experience and data protection needs
8. Enhance ease of use by unifying the management of accounts, passwords and access for all apps, both internal and external

include the loss of a device or the use of a device for malicious intent. Smith says that agencies should use Enterprise Mobility Management (EMM) and virtualization to address both access and security concerns.

65% of State and Local IT Managers say they expect the number of mobile workers to increase over the next five years.

Citrix "State & Local Mobility Map: Road to Mobile Readiness" Survey

EMM is comprised of technology solutions that manage the increasing array of mobile devices, applications and data access to enterprise services. This goes beyond traditional Mobile Device Management (MDM) solutions and includes BYOD and agency-supplied equipment. The addition of virtualization, allows enterprises to separate where an application lives from where the application is accessed. This improves accessibility of applications while maintaining a tighter level of control of the application and its associated data.

"People need access to a variety of applications to allow for maximum productivity. This can range from mobile ready applications, like email and web-based applications, but also includes enterprise applications — like case management or financial packages — that aren't entirely web-based or mobile-ready," Smith says.

The challenge for government is how to manage such a diverse environment while also meeting the growing needs for collaboration and data sharing, network management and virtualization. With the right solution in place, government agencies can build a mobile enterprise management portfolio that meets those needs, Smith says.

"Only then can we really meet the challenges of a mobile strategy that includes telework and BYOD as a priority to better serve citizens," Smith says. "Mobility has to be about improving department agility and productivity while providing secure access to things like apps and resources that are available anywhere and anytime."

Configuring Mobile Access for Government

Mobile productivity means freedom of choice and BYOD as an option

At the state and local level, employees are moving towards a new trend in mobile device usage — flexibility.

Right now, more than one third of all state and local agencies nationwide have matured their mobile strategy to a point where they are using formalized policies and practices. Often times Bring Your Own Device (BYOD) is an important part of that initiative, says Rob Breithaupt, a Sales Engineer on the public sector team at Citrix.

"Usually there's a choice involved, between a government-owned device or your own device," he says. "We're seeing agencies begin to develop their mobile strategy and focus more on a BYOD initiative. It's a way to meet employees who want flexible options when it comes to their own device."

Today, there are many people bringing their own devices to work. According to a Pew Research Center study, 64 percent of American adults now own a smartphone of some kind, making mobility a key entry point to the digital world. The pace of technology is only speeding up, and employees often work best when they're allowed to choose the device to use.

However, without a formal strategy for BYOD, government agencies face significant risks from security and compliance gaps to escalating IT complexity. BYOD policies can also help guide the decision making process for which employees receive government issued smartphones.

"For instance, some states give employees iPhones to those who want them. It's a government-owned device that's paid for by the state," Breithaupt says. "But then there are options like BYOD, which allow you to use your own device and plug into things like email, applications, and files remotely."

By embracing the trend of device consumerization, state and local government will meet the preferences of its employees, offering them newfound

productivity, mobility, flexibility and an enhanced work-life balance. But, there are a few things to consider when moving to a BYOD mindset.

First, there are new security measures to consider so that government data is secure and safe. BYOD brings a wide range of security, policy, and IT challenges that must be acknowledged and solved over time.

According to Breithaupt, it's a "you choose" approach that can result in greater work flexibility. There will always be the employees who are either required or choose to own a government device, he says, but increasingly there are more making the switch to BYOD.

64% of American adults now own a smartphone of some kind

Pew Research Center

"It comes down to making a conscious decision where the user decides the mobile experience that's right for them."

With BYOD Government Gains Access to:

1. *Any device, anywhere* — Employees gain the freedom to choose their own devices, including widely used desktops, laptops, tablets and mobile devices that run on iOS, Android and Windows-based software. There's also the advantage of seamless roaming and a single user experience across multiple devices, which helps ensure convenience and productivity at the same time.

2. *Desktop and application virtualization* — IT can transform any application as well as complete desktops into an on-demand service available to any device. The solution allows government users any combination of desktop and application delivery approaches to support every type of user through a single point of control.

3. *Secure file sharing* — Employees can securely share files with anyone and sync files across all of their devices. There's also the advantage of flexible storage options, policy-based control, reporting, data encryption and remote wipe to help keep government data and information secure.

4. *Self-service and remote support* — Staff can access any of their authorized apps, including Windows, web and SaaS applications easily on any device through a secure, consistent app store with a convenient single sign-on experience. IT can also centrally support people and technologies in any location to ensure uptime for PCs, Macs, mobile devices, servers and networks across the organization.

Accessing Government Data in Mobile Environments

California Improved Public Safety with Mobile Access to Data

By enabling mobile access to data, government agencies can work efficiently to deliver critical services to citizens. Mobility is how California is able to speed up the delivery of information to police officers, sheriffs, and probation officers working in the field across the state's 58 counties.

3+ devices are used daily by an employee for work activities.

Citrix Enterprise Mobility Report 2014

This access to data in mobile environments is giving many state agencies a new way to do business away from the office. In California, the justice system faced a key challenge:

How do you provide criminal offender records to a state network of officers, agents, and prosecutors in real-time?

The answer was mobility.

Police officers who worked beats used to rely on call dispatches to request and use Criminal Offender Record Information (CORI). But California, decided that this process was too slow for day-to-day police work. Government leaders created the Hawkins Data Center within the California Justice Information Services (CJIS) division and took a mobile strategy to operations.

"For the government field worker, this technology is essential," says Rob Breithaupt. "From just about anywhere, and at any time, these on-the-ground employees can access important apps like email, internal networks through a web browser, and file shares remotely."

It was any-network access to data that made all the difference for California's justice system. Thousands of DOJ personnel and their Law Enforcement Agency Partners (LEAPs) now use XenMobile by Citrix to secure access to web-based applications on government-issued smartphones and tablets.

"Each section of the department has its own

needs in terms of mobility, but the XenMobile solution fits the mold for every single one of them that we've encountered so far," says Tim Whitfield, Justice Mobile Systems Software Specialist with the California Department of Justice.

Our agents are much happier with the new solution... **People** in other departments now **want to work here** because we have this solution."

Chris Chambers, Deputy Chief Information Officer, California Department of Justice

Now, trial lawyers use iPads to access cases and other data, eliminating the need to search through large paper files. Special agents in the field can access criminal records on any authorized mobile device. And the data, which is hosted in DOJ's secure datacenter, is available to all partners, including state and federal agencies.

This mobile strategy has helped to bring government service up-to-speed. Previously, employees used laptops and wireless cellular adapters in order to access the department's virtual private network (VPN), a system that could take as much as 15 minutes to access.

Only 36% of employees are equipped with the applications they need for their job on the first day they arrive.

Citrix Enterprise Mobility Report 2014

With a mobile solution now in place, departments like the Bureau of Firearms, use data access to remove guns from the hands of criminals who are prohibited from gun ownership.

"That first weekend, our officers increased their productivity of running criminals through the database by 300 percent," says Chris Chambers, Assistant Bureau Chief for California's Department of Justice. "We've lost count of how many felony arrests we've made and illegal guns we've gotten off the streets because of our Citrix solution."

This is a mobile device management (MDM) solution that provides easy and secure access to data, Breithaupt says. "User experience is huge in the access and consumption of data. If at any point the mobile device becomes a pain point, then the employee is going to find alternative ways to get there."

The alternative, often times, is referred to as shadow or stealth IT — a process by which the user adopts his or her own technology for business use and without explicit organizational approval.

Take the example of online file sharing and access. Without a mobile, secure file share system, the employee may go around IT departments and download an application that is available on consumer-focused app stores, Breithaupt says.

"Users are not going to listen if they don't have the right technology solution. They will go find it themselves, and then you're putting your organi-

zation at a greater security risk."

In effect, the user goes rogue, and they download an application that puts the agency at risk to a security breach.

"File sharing applications are great products. Their functionality is great, but the main problem is control," Breithaupt says. "IT does not know where that file lives, or when it's being transferred."

ShareFile by Citrix is one of the enterprise data solutions that enables states to deliver on robust data sharing, helping to sync security with mobility needs.

In California, data sharing enables faster and more collaborative work to happen. Mobile security, which originally posed a challenge for the state's DOJ, is now an advantage.

The state's IT department shifted from a security mindset designed for traditional PC environments to a mobile security framework that eliminates the need for local data storage on a device. As a result, California has reached compliance mandates at both the department and FBI levels, Chamber says.

"Citrix provides the mobile device management capabilities we needed to achieve compliance, such as remote data wipe and the ability to control and restrict usage, while offering a great experience for our users."

Protect Sensitive Information from Loss and Theft

These are the top concerns when it comes to mobility

A crucial step for both employee and personal-owned devices is to protect data without impacting the overall user experience.

But, security isn't always top-of-mind for the individual using a mobile device. And, with new policies emerging, like BYOD, mobility must be balanced against the needs of security.

The public sector experienced nearly 50 times as many cyber incidents than any other industry in 2014, and cybersecurity remains a top organizational priority – 80 percent of state CIOs have adopted a cybersecurity framework based off of national standards and guidelines, and 87 percent have developed security awareness training for workers and contractors.

The smartphone or tablet that you hold faces specific security risks, says Rob Breithaupt. Devices can be lost or stolen, and there are malicious intent attacks directed at mobile devices.

In a recent Government Business Council survey, a majority of federal leaders said they had to sacrifice flexibility for security when it came to mobile device usage. For this reason, BYOD programs must include technologies to enable device-independent computing through enterprise mobility management (EMM).

"This is a complete enterprise solution for mobile device management and mobile application management," Breithaupt says. "It's a two-pronged approach that ensures government-owned and BYOD devices are controlled securely and safely."

Mobile device management (MDM) allows an agency to remotely wipe a device that is government owned without the permission of the end user. It's complete control over a device.

95% say they are 'concerned' about information contained in emails being stored on mobile devices.

Citrix Enterprise Mobility Report 2014

The difference comes with BYOD programs. Mobile application management (MAM) takes a step back from MDM and looks just at specific applications that will be accessing secure information on internal networks. This allows individual applications, such as email, live alongside personal applications. You can control business applications without impacting the other components of the smartphone, things like personal photos or email.

"In effect, the user gains secure access to all of their work-related mobile apps through a unified device, delivered across any network," Breithaupt says.

Most public sector agencies use some combination of device and application management for government-owned devices. While agencies that are making the move to device-owned mobility, mainly use application management, Breithaupt says.

A key to protecting sensitive information is to deliver it in a way that keeps the data off of the device. Solutions such as XenApp by Citrix can do this.

XenApp can also back-up data, protect intellectual property, and secure sensitive information. This solution allows for access policy enforcement, which can reduce the risk of an intrusion through unsecured connections and VPN holes. It establishes a service delivery architecture for apps leveraging common policies and tools that simplify deployment and management.

"Virtualization is the real differentiator," Breithaupt says. "Agencies are increasingly turning to hybrid clouds to deliver virtual infrastructure technology, storage infrastructure, and networking to a single platform."

This set-up also powers by solutions like the Worx Mobile Apps by Citrix, a suite of applications built from the ground up with security and user experience in-mind.

Virtualization solutions provide centralized control and management, flexible delivery, policy-based control, and endpoint protection. By leveraging virtualization as a security layer, the public sector can manage risk more effectively while providing optimal agility inside the business culture.

Reduce Cost and Simplify Management with Mobility

Empower your workforce with secure, seamless, and flexible options

With the move to mobility, the public sector is realizing several cost saving and management efficiencies, helping to empower work that is secure, seamless, and flexible.

"In the attempts to be more mobile, we often times build legacy systems that are duplicative and only provide levels of access," says David Smith, Director of State and Local Government at Citrix. "When you start out with the assumption that your end user is going to be mobile-first, a lot of what you build changes, and you can consolidate costs."

As Smith explains, there are two categories of savings: the hard ROI benefits vs. the soft ROI benefits of mobility.

"You can certainly add-up the infrastructure savings, but the soft ROI benefits, like worker satisfaction and productivity, that might be even greater," Smith says. "They're harder to measure, but we see those as transformative processes helping to change the nature of government operations."

Really, mobility is the experience of being productive on any device through the use of applications and access to data. This process of untethering from the office or desktop is a game changer.

It's even possible to calculate the value of productivity gained by using a mobile strategy. And, in a recent study on mobility, it was found that mobile-ready agencies gain three additional hours of productivity per week, per employee.

"Office productivity has become a real key in workplace culture," Smith says. "Mobility goes hand-in-hand with productivity and team collaboration."

He calls it the "your-time" method to collaboration. A type of work where employees gain the ease to work where they want. They're able to do this by working in online, collaborative environments, where teams can access files, project updates, and messages from a variety of mobile devices.

From a personal standpoint, mobility gives employ-

ees the freedom of choice. They can decide when and where they work based on what makes them feel most productive, which can also enhance their work-life balance.

And, there's a clear preference toward productivity. When it comes to a mobile strategy, most enterprise businesses say that productivity is ranked as the top priority (58 percent of respondents) followed by collaboration (51 percent of respondents).

"One of the most challenging things that government now faces is maintaining and supporting the workforce through business continuity," Smith says. "Many agencies are realizing that mobility can be a key driver and strategy for your business."

Advantages for the Mobile Workforce

By Connecting Enterprise Business, IT Departments Can Drive Value

Mobility means IT can help drive a positive cultural shift, impacting almost every employee in the workplace. Here are a few examples of how a mobile strategy can result in greater productivity by role:

IT Manager: By minimizing security risks with application and desktop virtualization, the IT team can provide the tools for employees to be productive and keep data secure when accessing the network from anywhere — even if they're connecting from the newest devices on the market.

Government Executive: Leaders can make it easier to access state data on multiple devices. This improves collaboration across state and local governments and enables collaboration between team members, regardless of their location.

Department Manager: Individual government agencies and department managers can increase productivity, collaboration, and retention. Their employees feel the benefits of a flexible work environment, as they can connect from anywhere and anytime.

HR Recruiter: Human resource departments can recruit the single best applicants for a job, no matter their location. Not only can a search expand nationally or globally, HR can also provide the added selling point of a flexible, mobile organization to entice recruits.

Facilities Operator: The flexibility of a work-life balance also affords management of building costs and expenses. As more employees are able to work outside of the office, or increase the utilization of space in an existing office with unassigned seating.

Government Caseworker: Mobility is a distinct advantage for the caseworker who requires the use of mobile applications to document information in an organized and secure fashion. In this case, mobility becomes part of their daily workload, allowing them to communicate and stay connected beyond the office.

CITRIX® Public Sector

Government organizations face a dual challenge: fulfilling their responsibility to protect and serve citizens—from security and disaster response to the administration of public entitlements—while meeting ever-tighter budgets to control the cost to taxpayers. This becomes ever more difficult as the complexity and volume of regulatory mandates, citizen needs and caseloads increase. Government organizations must be able to share and act on vital information as effectively as possible across functions, agencies and borders. Agencies must support government agents wherever they work, whether at a main or remote agency, at home or on the road, by providing reliable, high-availability access to resources. IT must also deliver data to multiple branch locations, often across state and national boundaries, and recover quickly from service disruptions. Content privacy and security are essential to ensure that confidential information is not compromised.

www.citrix.com/solutions/us-government