Solving the six massive mobility challenges in government

From federal to local, agencies at all levels must address core concerns to get more from mobile computing.

IBM

Introduction

In government, the challenges of mobile computing are as broad as the reach of agencies and as diverse as agency functions. Across federal, state, county and city departments, with responsibilities ranging from parks to police, building inspections to military intelligence, water treatment to public transit, today's government employees need to be mobile to deliver services. They carry with them their own devices, including smartphones, tablets and laptops. Each requires management to ensure compliance with regulatory mandates, security to protect sensitive data, and performance to conduct tasks efficiently.

As a result, IT departments at government agencies require enterprise mobility management (EMM) solutions that can function across all these areas, whether organizational, geographic, operational or technical. While many enterprise environments face some of the mobility challenges that governments handle, few businesses must address the sheer variety, scale, fragmentation and sensitivity of mobile issues that confront governments daily.

This white paper discusses mobility in government, ranging from mandates for the secure transmission of data and use of applications, to the need to ensure the privacy of citizens, to the complexity of supporting bring-your-own-device (BYOD) policies. It provides a framework of six operational and technical concerns that an effective EMM solution must address—along with use cases that illustrate how some government entities have successfully dealt with these concerns. It concludes with a detailed overview of IBM® MaaS360®, an industry-leading EMM solution designed to provide the full range of device, data and application management capabilities that all levels of government require for their diverse, rapidly growing mobile computing environments.

Mobility has benefits and pitfalls for government agencies

Mobility is critical for the productivity and efficiency of today's government workers. Consider the building inspector who needs to access construction code or zoning documents while out in the field. Returning to city hall is not an option. It's much faster to wirelessly access the necessary information on a tablet, proceed with the inspection, and turn the building back over to the contractor to move ahead with the next phase of construction.

To effectively support these types of use cases, many government agencies have transitioned from on-premises infrastructure to cloud. The cloud enables agencies to provide the specific applications and stores of data their employees need—plus applicable resources to the public—from any place at any time in a nimble and scalable way. Many agencies have instituted BYOD policies, especially on the state, county and city level, that allow their employees to use their own devices. BYOD brings with it a win-win for both employees and agencies: workers use their preferred means to stay productive on the go while government IT reduces equipment expenditures.

When it comes to measuring the success of mobility in government, the results have exceeded expectations. The Federal Chief Information Officer of the United States, in fact, declared in 2013: "The future for us is one where mobile is the default computing platform."[1]

Even with this success, however, government agencies must take a precautionary approach. If a data breach occurs and sensitive data is compromised, no one—especially elected officials—wants to appear in the headlines or be blamed for the lapse. So, to keep data safe and mobile devices under control, governments have instituted regulations and controls. And while breaches rarely occur, remaining in compliance with regulations is an ongoing challenge and concern for IT.

Meanwhile, agencies embracing mobility must continue to grapple with a number of issues. Their capabilities must incorporate new technologies, as in the case of the federal Department of Defense seeking to use personal identity verification cards to authenticate users logging on to mobile devices. It must be secure, as in the case of a sheriff's office needing to send encrypted evidence to a district attorney in a criminal investigation. It must be cost effective, for the municipal IT department that cannot cut back on services despite limited staff and a tight budget. And it must be easy to use, for the citizen who needs to access county tax records to provide a real estate agent with a property's history.

Address six core concerns to master mobility

The move to mobility aligns government with today's forward-looking businesses. A recent survey revealed that 97 percent of enterprises plan to either maintain or increase funding for mobility. Of those surveyed, 75 percent already use it for greater flexibility, 64 percent for greater productivity, and 41 percent for employee satisfaction.[2]

Unlike standard enterprise environments, however, government agencies are typically cost-conscious, making procurement practices more difficult. The desire to spend less on hardware, software and services adds to the appeal of BYOD.

Given the sensitivity of information in government, data security is of top importance when implementing BYOD. Whether for a military plan at the federal level, or a hospital's health records at the individual citizen level, IT needs a plan to properly address how that data flows, remains secure and stays in-house.

Government is an area where both benefits and vulnerabilities are far reaching, so a forest of regulation has grown up to protect and regulate governments, data, devices and practices. Yet even as vulnerabilities are addressed, data must remain accessible, and government work must be efficient. Ultimately, this leads to a focus on six areas of core concern for mobile computing infrastructures and operations: security, simplicity, speed, scalability, service and stability.

Mobility challenges in government

Key concerns	Challenges
Security	• The need to abide by departmental and industry-wide data security policies and regulations • Data breaches and leakages that create headlines and tarnish stakeholder reputation • The wide range of regulations that guide different agencies at federal, state and local levels • At the state and local level, an influx of personal devices used for government work • At the federal level, confusion about Impact Level of Federal Risk and Authorization Management Program (FedRAMP) certification and EMM system content classification
Simplicity	• Tight budgets, understaffed teams and resource constraints facing government IT departments • Increased complexity and risks resulting from managing multiple vendors and integrating diverse products • The need to simplify BYOD with easy configuration; a self-serve application catalog; and simple, secure file access
Speed	• Antiquated operations, including pen and paper processes that still dominate many agencies • Slow deployment of IT projects often requiring months or years • The need to overcome the lack of agility in large and diverse agencies with fast and simple technology deployments • A rapid increase in retirees driving the need to attract young workers and get them quickly up and running
Scalability	• Enabling multiple, diverse departments in an agency with capabilities specific to their needs and preferences • The geographic dispersal of workers even within an individual agency • The need to provide the necessary tools for temporary, often seasonal, workers required for short-term projects • On-premises servers that require additional servers and IT support resources to scale up
Service	• An overwhelming number of vendors, partners and technology products, prompting the need for simpler single sourcing
Stability	• The need for trusted partners to innovate, keep the cloud running, and provide support such as managed services • Reliance on federal security and risk management certifications for audits that each agency cannot conduct itself

Far-reaching needs call for a comprehensive EMM solution

IT organizations at government agencies have similar goals:

- Manage and secure their mobile devices, applications and data in a simple yet robust way
- Prevent data leaks
- Maintain regulatory compliance
- Empower employees to configure and use the devices with minimal IT support
- Protect the privacy, not only of their government users, but of the larger body of stakeholders—the citizens they serve

---

"This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information."

—Criminal Justice Information Services Security Policy[3]

In meeting these requirements, different agencies may need different capabilities from their EMM solution—for example, one agency might need a "container" approach that separates personal from work data and applications on the device, while another might need enhanced security to ensure that only privileged users have access to data on a central server—and enforce policies and practices to ensure that those users do not misuse their privileges.

What applies to all agencies, however, is the fact that each of these needs must be addressed using a comprehensive solution.

Security

The IBM X-Force® security team recently noted that computing environments for business and government alike today experience "an ever-upward trend of more attacks, more leaked records and more varied threats."[4] To defend against these attacks, government agencies need solutions, policies and practices that enforce secure operations for their total computing environment, including mobility. In providing BYOD capabilities for their mobile workers—an arrangement growing in popularity, especially with state and local governments—IT needs tools to cope with issues ranging from lost and stolen devices to users who download insecure and unapproved applications. At all levels, governments and their IT organizations need to comply with regulatory mandates designed to help ensure security.

Simplicity

The growing populations that governments serve, coupled with tight agency budgets and limited IT staff, make efficiency essential to achieving operational and programmatic goals. As agencies face pressures such as the need for data and infrastructure security and the desire to take advantage of rapidly expanding technology capabilities, simplification of their IT systems has become the key to achieving that efficiency. IT needs relief from the complexity that grows from dealing with multiple vendors, business partners, technology products, and supporting workers that lack technical literacy. These workers often prefer the familiarity of their personal mobile devices over agency-provided equipment, yet they may be uncomfortable with the need for IT to manage and secure their personal equipment for government use.

Speed

Transforming government operations—and doing it quickly in agencies that may be uncertain how to achieve change, lack resources for innovation and often have a reputation for moving slowly—can be a challenge. But rapid change, along with faster internal operations and external delivery of services, is the norm in today's business world, and it is increasingly expected in government, as well. Citizens expect smooth, unencumbered operations. With the huge baby-boom generation reaching retirement, public agencies seeking younger replacements need to provide the same dynamic, technology-driven, mobile environments these next generations have come to know in the private sector.

Scalability

As public services and internal operations evolve, governments not only face challenges in delivering them quickly, they can face challenges delivering them at the necessary scale. "Crawl, walk, run" is often the mantra of government, as change frequently starts with one team, then expands to one department before rolling out agency-wide. The need to do more with less is true in both agency budgets and IT staffing—and may result in a cautious approach. Yet growing cities, states and nations demand more. To scale their operations quickly, seamlessly and cost-effectively to meet this demand, governments are increasingly turning to cloud systems. Unlike other delivery methods, the cloud can easily expand and connect technology services across the infrastructure, from the mobile worker's BYOD smartphone to centralized mainframes in the agency data center.

Service

IT may be a key driver in creating and enabling change, including the move to mobility, but much of the IT team's work takes place behind the scenes. Seamless delivery of technology to the public and agency employees requires insight into the programs the technology supports as well as into the effectiveness of technology in delivering that support. As a result, requirements for continuously monitoring, diagnosing and remediating the performance of computing systems, including mobile devices and their users, are pervasive, especially when it comes to security. Federal Information Security Management Act (FISMA) requirements for federal agencies, for example, now require continuous monitoring of all endpoints and security data. In an environment that deploys mobile devices or allows BYOD, an effective EMM solution can significantly improve the ability to meet mandates and support programs.

Stability

Amid the rapid evolution of technology capabilities, the frequent and disruptive business changes—including acquisitions and mergers—that prompt change in technology vendors, and the volatile political and economic environments where government operates, agencies need stable and reliable ways to deliver public services. Mandates such as FISMA, which defines a framework for managing information security, and FedRAMP, which establishes a baseline for security assessment and continuous monitoring to reduce risk in cloud services, can help. An EMM solution can supply the insight and control agencies need for reliable operations using mobile devices.

How government entities are meeting mobility challenges

Key concerns	Use cases
Security	• In hospitals, tablets used at the point of care are securely shared among doctors, nurses and other healthcare workers through techniques including secure authentication, user settings and access controls. • At state or national park entry points or gift shops, a tablet put into kiosk mode securely prevents data leaks while accepting credit and debit card payments.
Simplicity	• A local government licensing and inspection agency institutes a BYOD program to support mobility when staff members are on location for audits and inspections. • The IT department configures personal devices with a data container for emails, calendar, contacts, web browsing and applications that secure the data—not the device—encouraging user acceptance of management.
Speed	• The City of Philadelphia's Community Life Improvement Program mobilizes field agents with smartphones to gather data and photographs to help improve neighborhoods through the eradication of blight such as graffiti. • The mobility program reduces the time for delivering location, crime and graffiti-related data and processing reports—formerly handled manually, on paper—from three weeks to near real-time.
Scalability	• A federal agency that relies on short-term but large-scale data collection quickly ramps up thousands of government data collectors and devices and quickly ramps down when project aspects are retired. • Data is collected on tablets and smartphones rather than paper notebooks or heavy laptops, with devices and applications communicating directly to a central cloud service.
Service	• A resource-strapped agency goes mobile with a complete solutions and services offering from a single provider to make its staff and its offerings to the public more efficient. • The comprehensive approach addresses the full mobility lifecycle from acquisition of devices to application and content access to device retirement.
Stability	• In a changing technology landscape, a federal agency relieves uncertainty about compliance by leveraging certifications provided by its EMM solution, enabling them to avoid conducting their own audits of cloud solutions.

Mobility mandates require better security and control

Regulations exist at all levels of government. The principal federal government and industry requirements, affecting government agencies and users equally across the county, include:

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA):** Applicable to programs of the federal Department of Health and Human Services and state healthcare and Medicaid programs. Establishes standards for protecting health information that is held or transferred in electronic form.
- **The Health Information Technology for Economic and Clinical Health Act (HITECH):** Also applicable to healthcare programs. Modifies the federal government's authority to audit HIPAA compliance and impose greater financial penalties for HIPAA violations.
- **Criminal Justice Information Services Policy (CJIS):** Applicable to individuals and agencies working with criminal justice services and information. Provides controls to protect the lifecycle of criminal justice information whether at rest or in transit; provides guidance for the creation, viewing, modification, transmission, dissemination, storage and destruction of data.
- **Payment Card Industry Data Security Standard (PCI DSS):** Applicable to any business or agency handling payments via debit, credit, prepaid card or other electronic means. Sets standards for ensuring the security of transactions, which in government can range from tax payments to collecting admission fees at a museum.
- **Federal Information Security Management Act (FISMA):** Applicable to information systems used or operated by a federal agency or by a contractor or other organization on behalf of a federal agency. Defines a framework for information security at these agencies, which is further defined by standards from the National Institute of Standards and Technology (NIST).
- **Federal Risk and Authorization Management Program (FedRAMP):** Applicable to providers of cloud computing services. Establishes baseline security assessment and continuous monitoring requirements for FISMA-defined risk levels using NIST standards for all cloud systems.
- **Federal Information Processing Standards (FIPS 140-2):** Applicable to non-military government agencies and contractors. Provides four levels of security covering areas related to the secure design and implementation of encryption of mobile data.

Speeding provisioning and boosting control

In sparsely populated Nevada, the Department of Transportation (DOT) has rapidly increased its use of mobile devices to improve communications among workers and collect data from far-flung equipment such as cameras and weather detection devices. But managing mobile devices from a central location was a challenge.

Replacing manual provisioning and support with MaaS360, a comprehensive EMM solution, the department was able to reduce imaging and setup time for each device by 30 to 40 minutes, followed by increased visibility and security management.[5] MaaS360 allows the DOT to see which applications are loaded on each device, blacklist unapproved applications, remove access to state data from devices that do not comply, and wipe devices clean if they are lost, stolen or create some other security hazard.

Reducing cost and increasing visibility

A government unit that manages purchases for other agencies found that the operational cost for its own mobile device infrastructure was high while its visibility into systems was low, due to the variety of management tools it employed. Among these were tools requiring time-consuming manual management for security, policy and compliance reporting.

Moving to cloud-based operations, the agency deployed MaaS360 to 16,000 endpoints in less than a week, while adding 6,000 agency-owned Apple iOS devices. Converging management allowed for retiring old systems while providing greater visibility into the agency's anti-virus protection, patches installed, encryption and firewall, with custom reports for greater insight into mobile operations.

Which EMM capabilities does your agency need?

An EMM solution allows government entities to enable and secure mobile devices, applications and content. In some cases, capabilities are similar to those in other systems management software. In other areas, however—as in controlling the download and use of applications—requirements can be significantly different.

NIST guidelines for mobility in defense agencies, in fact, contain nearly 300 "rules" that could be applied to EMM systems.[6] The following are key capabilities for managing mobility any government entity should have:

- **Central management:** From a single interface, managing policies for restricting the use of hardware features such as cameras, restricting the use of software features such as browsers and controlling the use of wireless interfaces such as Wi-Fi.
- **Data insight:** Monitoring and reporting on policy violations stemming from the device's access to and storage of data
- **Encryption:** Enforcing strong encryption for communications between devices and the agency, as well as strong encryption for stored data
- **Wiping stored data:** Fully or selectively removing data when a device is lost or stolen, or after incorrect authentication attempts
- **Authentication:** Requiring passwords and other forms of authentication, setting parameters for password strength and retries, and allowing administrators to reset access privileges remotely
- **Locking:** Forcing devices to lock after a specified idle period and remotely locking devices left in insecure locations
- **Application control:** Whitelisting and blacklisting applications, as well as installing, updating and removing applications remotely; distributing applications to users from an application catalog
- **Access control:** Preventing devices from synchronizing with local or cloud-based systems; preventing access to the network if a device has been jailbroken or rooted

"The true cloud-based MaaS360 approach is in perfect sync with our goals to reform IT management systems. MaaS360 will help reduce power consumption, secure data and reduce person-hours of labor, while successfully moving us away from legacy software systems."

—Office of a federal agency CIO

How IBM helps meet the challenges of government mobility

Key concerns	Solution features
Security	• Visibility and control over mobile devices, applications, documents and files from a single pane of glass • Automated policy enforcement for passwords and encryption • An automated, event-based, contextual rules engine for managing security policies and compliance • Ability to take remote action on nonconforming devices to ensure anytime, anywhere device and data security • Ability to remotely locate, lock and wipe (full and selective) mobile devices • Data container to separate personal and work email, contacts, chat, calendar, documents, applications and browsers • Secure access to back-end systems and databases with no need for a device virtual private network session • Real-time reporting, analytics and audit history
Simplicity	• Built-in and tested integration with solutions from IBM technology partners, providing a single mobility platform • Integration with IBM Security products, enabling IBM to serve as the agency's mobile platform • Ability for users to enroll mobile devices remotely (e.g., at home or in the office) without assistance from IT • A self-service portal that allows users to reset their own passwords and locate and wipe lost or stolen devices
Speed	• Cloud-based solution with seamless integration with the government agency's IT infrastructure • Fast setup: simply installing an agent, configuring portal settings and pushing out the application
Scalability	• Add one device or thousands seamlessly without having to add or manage servers • Quick deployment of application catalogs of both third-party and agency applications • Seamless integration with cloud and legacy government systems
Service	• A single point of contact for the device lifecycle—procure, activate, provision, manage, support, refresh, retire • IBM Managed Mobility Services available through IBM Global Business Services® for deployment of mobile projects • Support and implementation help included and available via chat, phone and email, or in person
Stability	• Deep IBM experience and expertise with government deployment of technologies and services • Impact Level 2 FedRAMP (FISMA moderate) certification earned that meets the needs of most government agencies; IBM does not store or host content on platform

Cloud-based MaaS360 delivers the security and control agencies need

Highly scalable and rapidly deployable to meet the mobility needs of government agencies of all sizes and areas of responsibility, MaaS360 offers comprehensive EMM capabilities in a cloud-based solution. Whether hardware is procured by the government agency or owned by the employee under a BYOD program, MaaS360 is designed to manage and secure devices ranging from smartphones and tablets to laptops and desktops, while delivering the applications and documents users need to be productive, without requiring the storage of critical government information on the MaaS360 platform.

"Increased mobility in the field is bringing major benefits to the city. Now that we can collect data from various sources, bring it together and analyze it in real time, we know what crime is happening where, and the city's decision-makers can best determine where to build a new facility or what actions to take in a certain neighborhood."

—Francisco Galarza, Mobile Computing Solution Architect, City of Philadelphia

IBM MaaS360 Cloud Extender enables plug-and-play operations with legacy government systems for simplified transition to the cloud. Agencies can securely integrate with their IBM Notes®, Microsoft Exchange, Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP), certificate authorities, and more in an easy plug-and-play fashion. Unlike other EMM solutions, MaaS360 Cloud Extender ties into back-end systems in a completely non-intrusive way and is not inline proxy with critical messaging flows, so it is not in the direct path of email.

The flexibility of MaaS360 allows government agencies to begin with essential, comprehensive EMM capabilities and layer on more advanced management tools quickly and easily as their needs grow. Regardless of the diversity of challenges and use cases your government faces, MaaS360 provides a stable, secure, simple-to-use management platform delivered by a single, trusted vendor.

"We found MaaS360 to be a strong and well-documented MDM solution for managing smartphones and tablets for employees and for allowing the use of personal devices to access town resources."

—Ajay Joshi, Chief Information Officer, Town of Gilbert, Arizona

MaaS360 provides instant access to a full production portal that gives IT administrators the ability to begin enrolling their first devices and recognizing value in minutes. Whether keeping government data and applications separate from the user's personal information to help build acceptance of a BYOD program among city employees, or providing secure, encrypted communications for a federal agency supplying data services to the military, MaaS360 delivers a necessary, protected and productive mobile environment for government agencies.

Conclusion

The growth of mobile computing challenges government agencies in six key areas: security, simplicity, speed, scalability, service and stability. With deployments in agencies at many levels of government including federal, state and local, MaaS360 has the credibility, reputation and trust with agencies of all sizes and with all areas of responsibility. Delivered and supported by a trusted leader in mobile management and security,

MaaS360 provides integration with leading security portfolios including the IBM Security Trusteer®, IBM QRadar® and IBM BigFix® families of products, as well as with leading solutions such as IBM Security Access Manager and IBM Cloud Security Enforcer.

MaaS360 is available to government agencies for a 30-day, no-cost trial. As agencies develop strategies and plans to effectively execute mobility programs, IBM can help along the way with both software solutions and services for advice, technical support and professional consulting.

For more information

To learn more and for a no-cost trial of MaaS360 software, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/maas360

[1] Wyatt Kash, "White House Announces Mobile Security Guidelines," *InformationWeek Government*, May 24, 2013. http://www.informationweek.com/regulations/white-house-announces-mobile-security-guidelines/d/d-id/1110120

[2] "The Massive Mobile Migration," *IBM Corp.*, April 27, 2016. http://www.slideshare.net/ibmsecurity/the-massive-mobile-migration

[3] CJIS Information Security Officer, "Criminal Justice Information Services (CJIS) Security Policy," *US Department of Justice*, October 6, 2015. https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

[4] "IBM X-Force Threat Intelligence Report 2016," *IBM Corp.*, February 2016. http://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03114usen/WGL03114USEN.PDF

[5] "Nevada DOT Implements iPad-Based MDM Solution," *Field Technologies*, October 2012.

[6] "*The Mobile Device Management (MDM) Server Security Requirements Guide* (Draft) Version: 1, Release 0.2, 18 July 2012," together with an overview memo, is available in a zipped file at: http://csrc.nist.gov/publications/PubsSPs.html#800-124 (Hit CTRL + F then type in "SP 800-124 Rev. 1"). The SRG document is in XML format.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
September 2016