IMPACT
Assessment

Mobility and the Federal Government

Ubiquitous mobile devices and applications have far-reaching implications — now and later — for IT and federal agencies.

To say mobile is mainstream doesn't seem to properly capture the picture of its rapid ascendancy and influence in modern life: Two out of three Americans now own a smartphone, according to the Pew Research Center. (It's also worth noting that 40% of them use their phones to access government services and sites.) The federal government is no exception, as many diverse agencies implement both proactive mobilization strategies as well as manage the inevitable growth of personally owned devices and apps popping up in government offices and field environments.

This impact assessment identifies several critical effects on federal IT as a result of massive mobile usage. Moreover, it highlights the considerable opportunities mobility offers to federal agencies and their workers, from increased agility and situational awareness for personnel in the field to better intra- and interagency collaboration and improved resource utilization and consolidation. The mobile era is both a present and future reality, with new waves of devices and applications expected to join ubiquitous smartphones and tablets in everyday use — so much so that our definition of "mobility" may need to be revisited.

Let's take a look at several significant impacts of mobility on the federal government, and how organizations can embrace the opportunities mobility creates while managing its inherent risks.

IMPACT: High Stakes for Information Security

Information security should be top of mind for just about any organization or individual these days. But the stakes are even higher for the federal government when you consider the enormous sensitivity of the data it generates and must protect, from the military and intelligence communities to the Internal Revenue Service to the Department of Health & Human Services and more. Mobility has exponentially expanded the threat landscape and attack surface with its proliferation of new devices and applications, plus the data they produce and store.

There's some good news here: A recent mobile security survey found that 66% of government respondents have some controls in place to identify and classify data. But that's not good enough, according to the report, which added, "Given the nature of government agencies — a breach could compromise national security — that number should be even higher." Just 27% of government respondents said they're able to prevent data from leaving secured devices.

Moreover, InformationWeek's 2015 Federal Government IT Priorities Survey found that 70% of respondents view cybersecurity and information security programs as "very important" to their agencies. Yet the report notes that "while our survey indicates that government agencies have a sharp eye on information security, they're falling behind in critical areas such as cloud, data center consolidation, and overall IT innovation."

In concert with the emphasis on security, federal agencies — and their vendors — must also manage a wide range of regulatory standards and compliance mandates. This is certainly an important factor when deploying new technologies, selecting vendors, and creating policies that govern mobile users.

IMPACT: Increased Need for Agile, Scalable, and Secure Infrastructure

Mobility is, of course, about much more than managing risk and compliance. It should also be about new opportunities. The proliferation of new applications and the potentially massive amounts of data they produce require flexible,

> **Most government IT professionals believe security is crucial, yet only about one in four has any way to prevent data loss on employee devices.**

highly available, and — you guessed it — secure infrastructure resources.

Enter cloud computing, virtualization, and mobility management technologies, which can drive desktop and device costs down, enable shared services and resource consolidation, reduce data security risks, and improve continuity of operations (COOP) and disaster preparedness, among other benefits. Data center consolidation alone can cut IT costs 50% to 70% by consolidating resource pools and delivering highly available machines via thin clients and mobile devices.

Better still, unlocking the power and potential of cloud, virtualization, and mobile technologies can enable federal agencies to improve employee productivity and agility through secure data access, better training opportunities, and enhanced collaboration among different teams and departments. And it's all highly scalable, enabling IT to bring new virtual machines and applications online with greater agility and efficiency — a need that's likely to grow as new kinds of devices and applications ultimately make their way into agency operations over time.

Consider field operations, a common-yet-critical scenario where mobility, backed by cloud and virtualization platforms, fosters tremendous opportunities and efficiencies. By allowing remote workers, including military personnel, to seamlessly access real-time information, content, and applications securely from any mobile device, federal agencies can improve productivity, response time, and reporting from a variety of field environments.

IMPACT: Preparing for Mobility's Continued Expansion

If you think mobility is pervasive today, just wait: It's poised for considerable growth, and so are its impacts on federal IT. Research firm Gartner, for example, included "Computing Everywhere" in its Top 10 Technology Trends for 2015 list. Gartner's David Cearley wrote: "As mobile devices continue to proliferate, Gartner predicts an increased emphasis on serving the needs of the mobile user in diverse contexts and environments, as opposed to focusing

MOBILITY, CLOUD, AND COMPLIANCE

Mobility and cloud technologies go hand-in-hand. Legacy-software approaches to client computing simply can't keep up with the demands of modern mobility. There's a reason, for instance, that "cloud/client computing" has been a regular on Gartner's annual technology trends list: "The convergence of cloud and mobile computing will continue to promote the growth of centrally coordinated applications that can be delivered to any device."

Indeed, cloud — like virtualization — is one of the related technologies that creates and unleashes mobility's vast potential: It can enable fast, real-time access from anywhere, at any time, keeping personnel connected, productive, and agile. Meanwhile, federal agencies can reduce costs, redundancies, support burdens, and other issues.

Yet just 11% of respondents in InformationWeek's 2015 Federal Government IT Priorities Survey listed cloud initiatives as "extremely important," with 57% rating them as "moderately important." And nearly half (46%) said their agencies have no cloud projects on the books for the coming fiscal year, which actually represents a 5% uptick from the previous year.

The transition into the cloud environment hasn't always been a smooth one for federal agencies, yet the cloud offers significant potential in terms of security, compliance, resource utilization, and consolidation. In fact, the Federal Risk and Authorization Management Program (FedRAMP) was specifically created to address those challenges, encouraging cloud adoption while standardizing how agencies manage security assessment, authorization, and monitoring of cloud services. FedRAMP's goal of reducing redundancies and waste — saving 30% to 40% in costs as a result — meshes well with the big-picture opportunities afforded by mobility, virtualization, and cloud. Similarly, the federal Cloud First policy and Federal Cloud Computing Strategy mandates will also help drive interest in and adoption of cloud technologies by government agencies.

VMware's vCloud Government Service can help, offering a FedRAMP-compliant hybrid cloud for deploying and running government applications in a secure manner.

> **"Mobility is an enormous opportunity that doesn't need to involve security trade-offs. Consider how secure, real-time access to data and applications can enhance the agility and productivity of field and remote workers."**

on devices alone."

Indeed, imagine the implications and opportunities of mobility's broadening horizon for federal agencies and personnel. Strategic mobility should engender better interdepartmental collaboration, agency productivity, and mission accomplishment. A highly available, secure, and scalable approach to infrastructure and applications will grow more critical by the year.

Even as federal agencies currently bring their mobile and related strategies up to speed, the next drivers of new devices and applications are already underway: wearable technologies and the broader landscape of the Internet of Things (IoT), the latter of which was a hot topic at the recent Federal Mobile Computing Summit. And for good reason: Almost across the board, analysts predict massive IoT growth, both in terms of dollars and in terms of the number of connected "things." Connected is the operative word: Forrester analyst Jennifer Belissent, for one, suggested in a recent blog post that "connectivity" may be a more accurate term than "mobility" as more and more data and applications come online.

Envision the potential for new wearable devices for military personnel or the possibilities of new health sensors in Centers for Disease Control (CDC) environments. Citizen demand for IoT applications that interact with government services seems likely to grow, too. In just about any government agency or office, the potential applications of IoT appear vast — and bring corresponding impacts of this expanding mobility and connectivity on IT. As IDC Senior VP of Research Vernon Turner noted recently, IoT will generate a new deluge of data from many more devices connecting to networks. "The Internet of Things will give IT managers a lot to think about," he said.

No matter the possible IoT or wearable scenario, all federal agencies will need to manage a common outcome: continued, explosive growth of data that must be managed, stored, and secured.

Proactive planning and innovation will give federal agencies a leg up as the next booms in connected devices and applications occur. Yet the fundamentals and lessons learned from mobility's current impacts will likely remain the same: You'll need the right mix of technologies and strategies to capitalize on potential gains in response times, employee productivity, cost savings, waste reduction, communication and collaboration, transparency, and other areas.

BOTTOM-LINE IMPACT:
How VMware Can Help

VMware Workspace™ Suite offers a purpose-built mix of virtualization, collaboration, and enterprise mobility management (EMM) tools to help capitalize on mobile opportunities both in the office and in the field. The suite enables employees to access their applications and data in a single, digital workspace — anywhere, anytime, from any device. IT, meanwhile, retains full control over users, access, applications, and data, ideal for managing a mobile workforce across multiple locations, device types, cloud environments, and so forth. IT can manage all of this from a single, centralized Web interface.

This solution increases overall IT efficiency while cutting costs — a common, recurring demand in federal agencies — in a variety of ways:

- Centralized desktop and device management reduces costs.
- Support for thin clients and zero clients decreases total cost of ownership.
- Automated provisioning, patching, and updates for desktops ease support and maintenance burdens while improving endpoint security.
- Virtualized infrastructure and desktops, along with cloud computing, foster high availability and seamless access to applications and information in disaster scenarios.
- Organizations can manage and secure all mobile devices, regardless of type, platform, or ownership, from one central console.

From a data security and integrity standpoint, VMware Workspace Suite enables advanced security features for any device type or use case. Data always resides on servers behind agency firewalls — not on the devices themselves — and role-based access controls, multifactor authentication, and identity management provide granular control of employee and contractor access to data and apps. Meanwhile, end-to-end EMM security capabilities extending to users, devices, applications, content, data, email, and networks include advanced data loss prevention (DLP) features and automated compliance monitoring and remediation on mobile devices.

Mobility is no passing fad. The utility it provides is what has driven its phenomenal adoption, and this utility will provide even more opportunities for applications for government workers. Will your agency be ready to capitalize? ■

ABOUT VMware

VMware is a leader in cloud infrastructure and business mobility. Built on VMware's virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant, and more secure. Customers can innovate faster by rapidly developing, automatically delivering, and more safely consuming any application. With 2014 revenues of $6 billion, VMware has more than 500,000 customers and 75,000 partners. The company is headquartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com.