

Online report
sponsored by:



Mobile & Wireless

Inside

Employees Can't do their Jobs Effectively Without Their Mobile Devices	s2
The Case for Enterprise Apps	s5
The Rise of the Tablet	s7
Mobile Device Management: A Prerequisite for BYOD	s9
Dismantling the Barriers to Increased use of Mobile Devices	s11



Employees Can't do their Jobs Effectively Without Their Mobile Devices

As more and more government departments allow or even encourage employees to use smart phones, tablets and other mobile devices to perform their jobs in or out of the office, everyone involved is beginning to see just how beneficial they are. Not only do mobile devices increase employees' productivity and effectiveness, but they further enable telework and otherwise increase employee satisfaction.

These are some of the findings of a new survey of 243 federal, state and local government respondents on the use of mobile devices and wireless networks by the 1105 Government Information Group. (Details about the methodology and demographic information on the respondents are below.) A study of the responses revealed that more than 40 percent of agency employees use mobile devices to perform work-related tasks. Furthermore, more than half agree with the statement that "our agency's

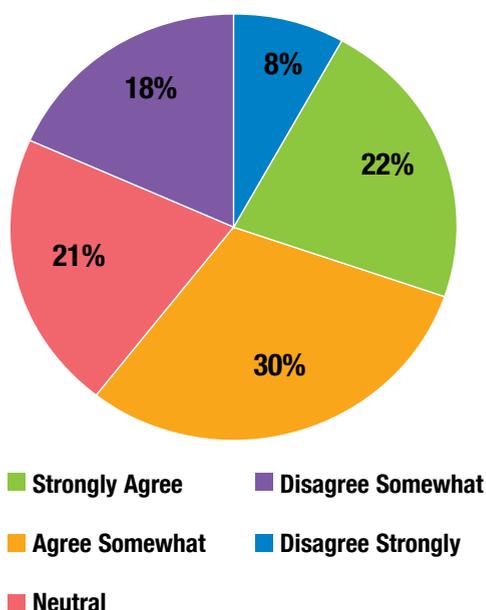
employees cannot do their jobs effectively without using their mobile devices" (see Figure 1).

The survey also found that the use of smart phones, tablets and other mobile devices is pervasive at all levels of government. In fact, the vast majority of senior agency executives and IT professionals are using them frequently for work-related activities (see Figure 2).

"We've had mobile devices in government for about a decade, but in the past couple of years, the applications and devices have become much more sophisticated, and a richer set of tools has been developed and deployed," says Chris Smith, formerly CIO at the U.S. Department of Agriculture and now U.S. federal chief technology and innovation officer at Accenture Federal Services. "At the same time, there are more applications for them, and agencies have come up with some very productive ways to take advantage of the capabilities."

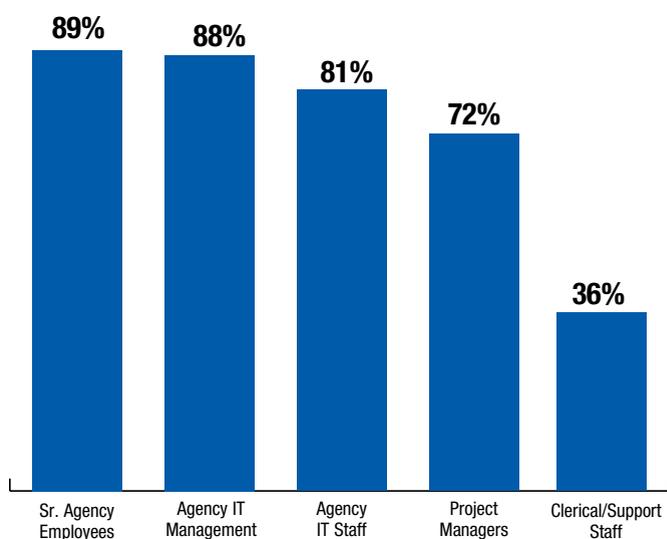
HEAVY RELIANCE ON MOBILE DEVICES

% of respondents who agreed, disagreed or had no opinion about this statement: "Our agency's employees cannot do their jobs effectively without using their mobile devices"



MOST MANAGERS AND IT STAFF USE MOBILE DEVICES DAILY

% Of respondents who indicated that the personnel used a mobile device daily for work related activities.



Battlefield smart phones

By being able to access context-based information in the field, for example, infantrymen can quickly retrieve maps, troop locations and even the location of hazardous devices. The result is a safer warrior who can efficiently and effectively execute missions in the field. It's happening already: Soldiers in the 10th Mountain Division will take smart phones with them to Afghanistan in the fall of 2012 that can record and broadcast the positions of explosive devices and monitor force positions, according to media reports.

Border patrol is another area ripe for the improved mobility of smart phones and tablets relative to laptops and other prior generations of mobile devices. If border patrol personnel see suspicious activity and are trying to determine if it is just illegal immigration or drug-based, they could access a mobile application that shows them past patterns of illegal activity in the area. Using predictive analytics (a form of business intelligence) accessible via a cloud, border patrol personnel could then make an educated guess about the type and severity of the threats and implement the appropriate response. By resolving the issue at the source, the government saves resources and protects American citizens.

There are also many benefits to public safety workers using a smart phone or tablet to dramatically improve productivity. For example, forest firefighters could access the latest data on weather, burn patterns from satellite imagery, logistic supply points and the location of other firefighters when rushing to an alarm. Similarly, building or construction managers could access blueprints without having to travel back to the office, Army Corps of Engineers planners could access complex imagery and 3D views of terrain in the field, and aviation and food safety inspectors could prepare and file reports in real time from the field.

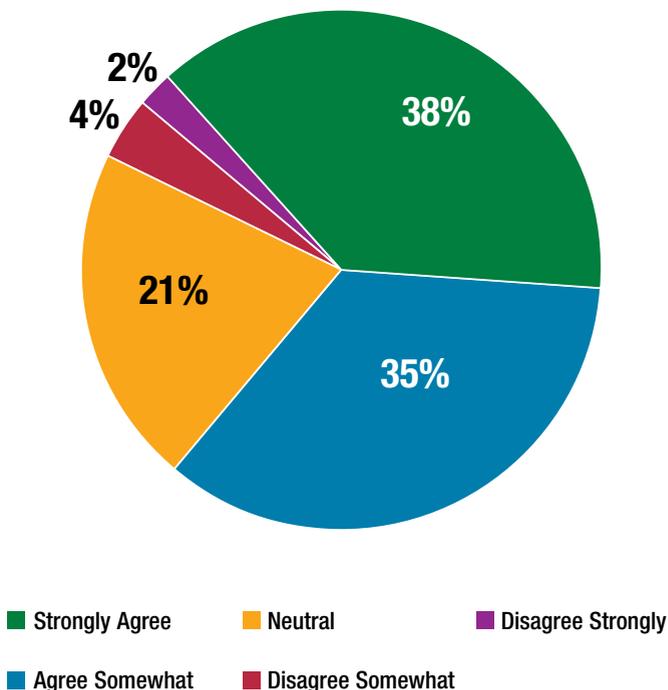
Government knowledge workers and their managers also can greatly benefit from using a mobile device while outside the office. With the ability to access critical operational applications (logistics, HR, budgets, program databases) on mobile devices, they can save time and increase productivity. Just the ability to make airplane and hotel reservations for a conference or off-site meeting, file an expense report, or approve an employee's timesheet via mobile phone or tablet is a major productivity enhancer for an executive. Access to e-mail and the ability to open attached documents helps attorneys respond to motions and requests more quickly.

The right mobility environment enables more telework

Working from home is considered a major employee benefit that also enhances overall productivity, and almost

MOBILE CAN ACCELERATE SHIFT TO TELEWORK

% of respondents' reactions to this statement:
Access to more robust mobile and wireless solutions will make teleworking an attractive option for our agency employees



three-quarters of the survey respondents indicate that faster wireless networks and more capable devices will sharply increase the appeal of telework (see Figure 3).

Josh Sawislak, a senior fellow at the Telework Exchange, a public/private partnership focusing on the federal telework and mobile community, says mobility is absolutely critical to the growth of telework throughout all levels of government. More than half of federal agencies are doing what it takes in terms of enabling the growing mobile workforce through telework, he says.

What's more, the ability to telework, enabled by mobility, is critical for recruitment and retention of top talent. That's particularly important as experienced federal workers retire and must be replaced with top candidates, he adds.

All these benefits collectively make the government much more productive. A recent study from MeriTalk on mobile-powered government concluded that if mobility enables federal workers to be just 10 percent more productive, the federal government could see \$2.6 billion in new productivity by 2013.

50% INCREASE IN ENTERPRISE APP ACCESS IN 2 YEARS

% of respondents who indicated they would use their mobile device at least twice a week for each of the following functionalities



“Productivity depends on job function, but there is no doubt that mobility makes government workers and, by default, government agencies more productive in general,” said Steve O’Keeffe, founder of MeriTalk, an online government IT community.

Beyond e-mail

Managers’ and professionals’ use of mobile devices for basic tasks such as e-mail is a good first step to increasing productivity, but the bigger benefit comes when these devices are able to access sophisticated operational

applications.

The survey found that although e-mail, phone and calendaring are currently used by almost all employees with a mobile device, access to enterprise-class applications will be increasingly common within two years. In fact, respondents predicted that their use of their mobile devices to access enterprise applications will increase by more than 50 percent within the next two years (see Figure 4).

“The low-hanging fruit is e-mail and being able to connect back to your files,” explains Accenture’s Smith. “But where you really find the benefit is when you can use mobility to solve operational problems. That means higher levels

Methodology and survey demographics

Beginning in May 2012, the 1105 Government Information Group launched a survey to better understand the use of mobile devices by federal, state and local government personnel. Subscribers to the 1105 Government Information Group’s publications, including Federal Computer Week and Government Computer News, were contacted via e-mail to participate in an online survey if they were qualified to participate by virtue of purchasing or managing mobile devices or wireless networks.

Of the 243 qualified respondents, roughly 50 percent work for a civilian federal agency, one-third work for the Defense Department or a related agency, and the remainder work for state or local governments.

Approximately one-quarter of the respondents are program managers or directors or in another type of non-IT role, while 73 percent are considered technical decision-makers, typically IT managers. And 55 percent characterized their agencies as relatively conservative when it comes to adopting new technologies.

of complexity and putting different pieces of information together. Often, it requires a combination of off-the-shelf apps, custom apps and social media.”

Smith elaborates on his vision with an example.

“If you are in economic development and trying to connect a bank with a start-up, you would have to have access to their underwriting engine, business plan and maybe a collaborative set of capabilities that lets them

evaluate local banks,” Smith explains. “If the business is a vineyard, for example, can you connect them with a bank, the technical support they need to have a solid business plan and prepare documents for the Small Business Administration? It’s all possible today with the right apps and the right workflow around it.”

Small devices with big budgets

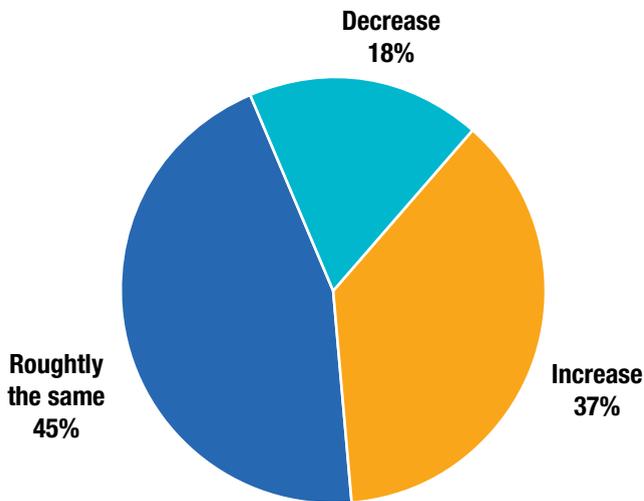
All this significant opportunity to improve government operations has persuaded agency leaders to allocate substantial new funding to take advantage of it. The survey found that roughly 15 percent of government IT budgets is allocated to mobile and wireless projects. Furthermore, more than one-third of government agencies have proposed budget increases for mobile and wireless solutions in the next 12 months. In fact, the overall average increase in mobile and wireless spending is forecast to exceed a robust 15 percent (see Figure 5). This spending is likely to occur in enterprise application development and security and otherwise enable greater mobile deployment.

Indeed, spending on improving the security of mobile devices with access to agency databases and other sensitive information is a high priority because of the importance of resolving the problem to encourage even more use of mobile devices.

Other articles in this “Download” explore the security challenges and solutions and drill down into the future importance of providing access to data center applications and data. Together, the survey and this study provide government managers with a road map for a successful trip on the mobile express. ●

ROBUST GAINS AHEAD FOR MOBILE IT SPENDING

% of respondents who indicated a specific change to their mobile and wireless IT budgets in the next 12 months



The case for enterprise apps

Given the strong focus on productivity, cost savings and efficiency, it isn't surprising that more and more government agencies are moving from application development focused on their desktop devices as the user access point to one focused on developing apps that will work equally well on any type of mobile device.

The benefits of moving enterprise applications to a mobile app environment are clear: They provide easy, fast universal access to whatever device an employee chooses to use and whatever location the employee is in. Apps can be developed once and reused continuously, and agencies have full control over access privileges. In turn, having access to these apps makes employees more productive, business processes more efficient and decision-making more accurate.

These benefits make enterprise apps a ripe area for growth. According to a new study by the 1105 Government Information Group, development and use of enterprise apps are poised for 50 percent-plus growth rates over the next several years.

Specifically, although four out of 10 survey respondents said they access enterprise apps via their mobile devices at least twice a week, in two years, more than six out of 10 will be using them. In addition to the sharp interest in accessing

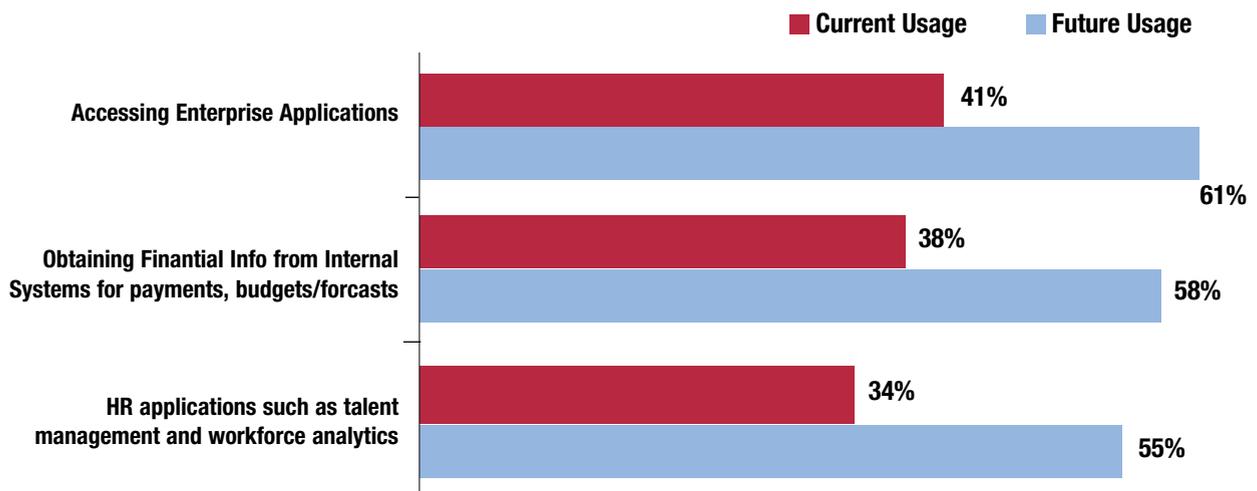
agency-specific enterprise apps via a mobile device, survey respondents also reported high expectations that they will increasingly access HR, finance and other standard back-office applications via their mobile device within the next few years (see Figure 1).

Enterprise apps work well in any category, including time and attendance, personnel management, logistics tracking and management, and business intelligence. Virtually every federal and state agency and department now has a host of enterprise apps:

- The U.S. Army has about a dozen mobile training applications for use on iOS devices, according to published reports.
- The U.S. Department of Agriculture has many as well, including expense management, payment management and business intelligence, according to Government Computer News.
- The National Oceanic and Atmospheric Administration is one of the biggest users of enterprise apps to date. It moved its 25,000 employees and contractors to Google Apps for Government, giving them collaboration and communication tools accessible on the go, according to Federal Computer Week.

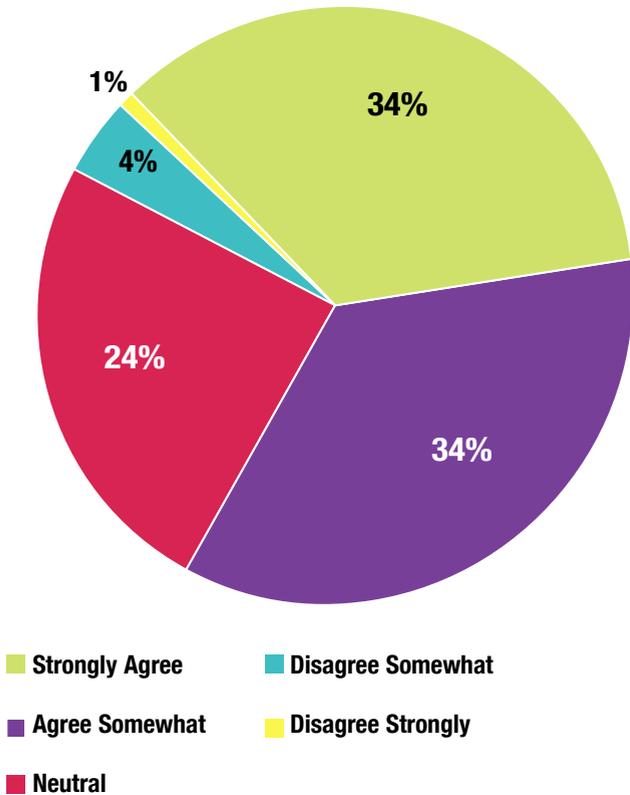
50% GAIN IN ACCESS TO ENTERPRISE APPS

% of respondents indicating use of mobile device to access different types of applications



HIGH DEMAND FOR AGENCY-SPECIFIC APPS FOR MOBILES

% of respondents who agreed with the statement that there should be a mobile apps store offering apps specifically designed for agency employees



using the latest version of apps, as well as relevant security patches.

According to the survey, 68 percent of respondents indicated that there should be mobile app stores offering apps specifically designed for agency employees (see Figure 2).

“Enterprise app stores increase security if only by virtue of cutting down the number of applications available to users,” said Steve O’Keeffe, founder of MeriTalk, an online community for government IT. “In many cases, they can also minimize the problems created by the diversity of devices, deploying the same application to nearly any device regardless of the underlying operating system. If device security and diversity are the problems, enterprise app stores are the right answer.”

Mobile app stores can offer both off-the-shelf apps from vendors such as Oracle and Google and custom-built apps. Customized apps are designed to fit the specific needs of the user base. For example, a Defense Department-focused app store would include apps for use on the battlefield and would comply with all DOD and federal regulations.

Many agencies today are starting enterprise app stores that include both types of apps. The U.S. Army, for example, has launched the Army Marketplace, which includes a host of training apps and a forum for Army personnel to request apps. NASA’s apps@NASA is starting slow, just offering basic apps such as time tracking, but media reports indicate it plans to expand its offerings soon. Both the Defense Information Systems Agency and USDA are working on mobile app stores, according to Government Computer News.

While enterprise app stores are starting primarily as tools of control — a way for agency IT departments to define the applications available to user devices and the associated policy — they will expand from that focus over time.

“The first path agencies could take is much like where we are today, with IT essentially stuffing mobile devices back into the client box and resuming strict control over how applications are developed and implemented at the agency,” O’Keeffe says. “The second path is more interesting and includes user input on what apps to include in the enterprise store and even extending to what apps get developed and implemented at the agency.” ●

Nuts and bolts

As the demand for access to enterprise apps grows, agencies have begun questioning how to best distribute and secure applications. For most, the solution is to build a customized enterprise app store, which allows users to download apps while giving agencies the ability to control access based on a variety of factors, including job function and security level. It also ensures that all employees are

The Rise of the Tablet

According to the 1105 Government Information Group’s May 2012 survey, 58 percent of mobile device operators in government use tablets, 89 percent use smart phones, and 64 percent use notebooks. What’s more, tablet use in government is expected to grow quickly over the next few years, in large part because of the devices’ versatility and lower cost (see Figure 1).

“I’m hard-pressed to think of a situation where you wouldn’t want to use one,” says Phil Simon, a frequent speaker and author of “The Age of the Platform: How Amazon, Apple, Facebook and Google Have Redefined Business.” “They have applicability for executives, traveling employees, telework and field workers.”

At the 2012 Government Mobility Conference, Gartner Vice President and Distinguished Analyst Ken Dulaney outlined the reasons for the growing use of tablets. Tablet prices will fall to under \$300 for entry-level units by 2013, and high-density screens will become mainstream. What’s more, the new Windows 8 operating system to be released in October could unify tablet and PC platforms within a year.

In addition, features on tablets continue to improve. More sensors, more powerful processors, better cameras and higher-resolution screens are coming soon.

Part of the reason for the expected uptick in tablet use is the rapid growth in activities other than e-mail, phone and calendaring on mobile devices throughout government. The survey found that accessing enterprise apps on mobile devices will rise by about 50 percent within two years. It also found that human resource applications such as talent management and workforce analytics would increase dramatically as well (see Figure 2).

Accessing enterprise apps such as financial reports is a much better user experience via the larger real estate and onscreen keyboard of a tablet rather than a smart phone, says Josh Sawislak, a senior fellow at the Telework Exchange, a public/private partnership focusing on the federal telework and mobile community.

“Tablets are ideal for reviewing and approving documents, accessing applications, taking notes in meetings, and anything that involves maps or graphics,” Sawislak says.

Tablets also can significantly increase the productivity of executives and managers. In addition to using the devices for approvals, reviewing e-mail and taking notes at meetings, they can even be used for decision-making when users are given the ability to access enterprise apps such as business intelligence and data on tablets.

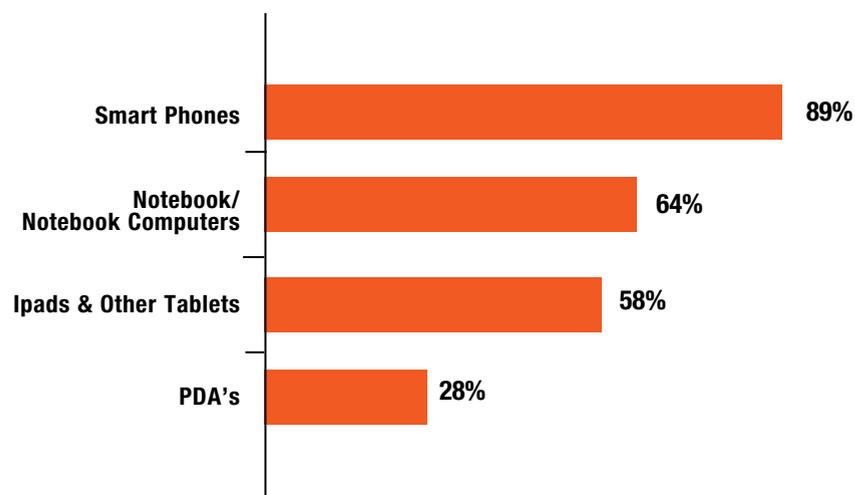
However, the value extends beyond the corner office. Tablets have proven especially useful for field service

personnel, many of whom must access large amounts of text, maps and other graphics-intensive applications. Building inspectors and construction managers, for example, need to consult detailed plans while on the job. Food inspectors must be able to access rules and regulations that would be difficult to read on a smart phone but in a form factor light enough to carry easily. The use cases are endless and include health care professionals, law enforcement officers, investigative teams and customer service personnel.

That’s not to say that tablets are appropriate for every kind of task and interaction — at least not yet. Although tablets are excellent for consuming information, they are less

MOST POPULAR MOBILE DEVICES

% of respondents indicating use of a mobile device at work



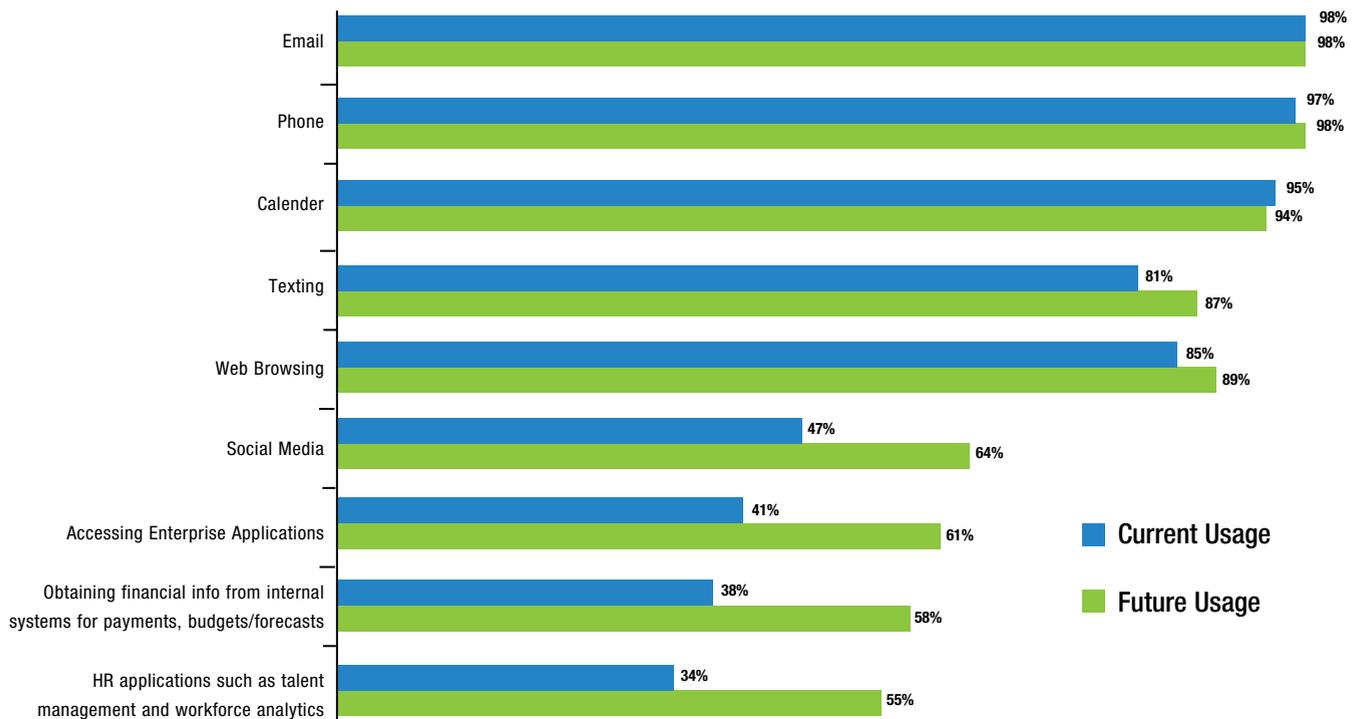
adept at creating information, such as full documents or complex analysis.

However, the ability to create content on a tablet will improve, Sawislak contends, as the notebook and tablet slowly begin to morph into one device that combines the best of both worlds. It's already happening; some notebooks are now designed with the same type of solid-state hard drives that tablets use, and tablets are gaining highly sought-after features such as 4G wireless connectivity, more powerful operating systems, larger screens and high-definition displays.

Within five years, Sawislak expects the tablet and notebook to merge. When that happens, the resulting device will become the device of choice, he predicts. ●

GROWING USE OF MOBILES TO ACCESS ENTERPRISE APPS

% of respondents indicating use of a smartphone, tablet or other mobile device for the following job-related tasks



Mobile Device Management: A Prerequisite for BYOD

Most government agencies that plan to increase their mobile spending in the next year are likely to encourage employees to use their own mobile devices at work — a practice that is commonly called bring your own device (BYOD). That finding, from the 1105 Government Information Group’s 2012 survey, masks the big picture, though: Government adoption of BYOD lags behind that of private industry.

“There is strong interest within the federal government for implementing BYOD, but it will likely lag the earlier and broader adoption we are seeing within industry,” says Chris Smith, formerly CIO at the U.S. Department of Agriculture and now U.S. federal chief technology and innovation officer at Accenture Federal Services.

“Organizations have figured out that they can’t stop people from bringing mobile devices into the workplace, so they might as well try to embrace it,” notes Phil Simon, a frequent speaker and author of “The Age of the Platform: How Amazon, Apple, Facebook and Google Have Redefined Business.”

To date, few government agencies have adopted BYOD, though several don’t bar employees from using their own smart phone or tablet at work. The vast majority of survey respondents indicated that their agencies provide devices to employees; just 12 percent of the respondents encourage a BYOD program (see Figure 1).

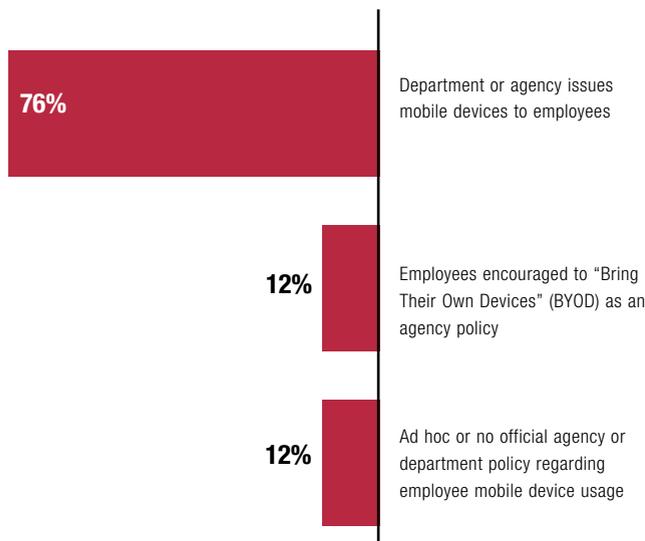
BYOD advocates cite many advantages for agencies that adopt such a policy, including the obvious device cost savings, increased productivity of employees using devices they already have and the reduced training costs, among others.

However, allowing employees to use their own devices for work-related tasks does have a cost. What if an employee with critical information on a mobile device forgets to back up the device? Suppose an employee loses a device with critical information on it or leaves the department suddenly?

These concerns are completely valid. The best way to ensure that these issues don’t damage the organization, the state or the country is by developing a comprehensive mobile device management strategy that includes not only

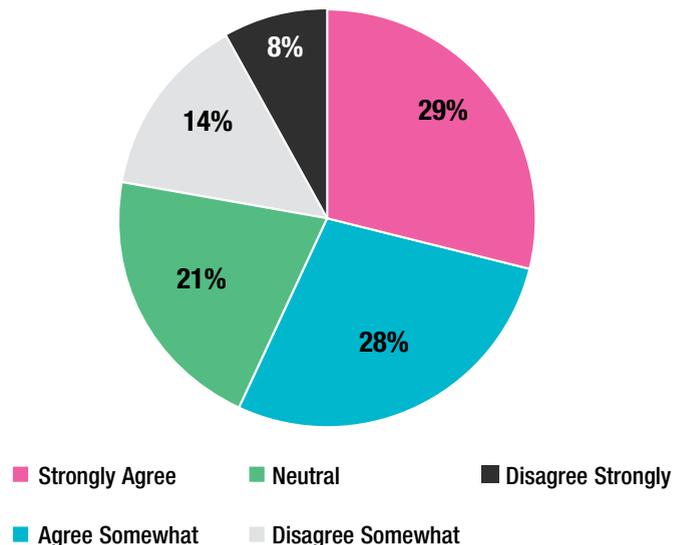
NOT MUCH BYOD--YET

% of respondents indicating specific policy about providing devices



SECURITY PROCEDURES DETER BYOD

% of respondents who indicated their level of agreement or disagreement with this statement: “Many of our employees don’t want to use their own mobile devices for agency business because of special security procedures”



policies and procedures but technology to back them up.

There are many types of tools on the market:

- MDM (mobile device management) solutions focus on securing the devices themselves.
- MAM (mobile application management) solutions secure applications used on mobile devices.

According to the survey, the most important parts of a mobile device management strategy are:

- Enabling network access from mobile devices via a secure virtual private network.
- Developing policies on which applications and data can and can't be accessed by employee mobile devices.
- Enabling the IT department to remotely wipe only agency apps and data from a device (leaving personal data alone).

Other best practices include requiring employees to use a

screen-lock passcode, enabling the IT department to audit devices for security compliance, encrypting all user data, and creating containers (sometimes called sandboxes) within devices that hold only agency data.

As important as these measures are, they can backfire if not done in a thoughtful and effective way. In fact, the survey found that by imposing too many security features and making it too difficult to use the devices, more than half of employees are deterred from wanting to use their own mobile devices for work (see Figure 2).

“One of the biggest challenges is how to put enough controls and security around sensitive data on a mobile device while still making them accessible and useful to employees,” says Smith. “Doing it right means having clear, thoughtful policy discussions.” ●

Dismantling the Barriers to Increased use of Mobile Devices

Although it is clear that mobility is the key to productivity, employee satisfaction and potential cost savings in government, several challenges have slowed adoption as agencies devote increasingly more attention and funds to resolve the issues. Cost, lack of clarity about regulatory compliance and IT integration issues are serious concerns for the vast majority of the 243 respondents to the recent survey by the 1105 Government Information Group. But security risks overshadow all the others.

Six out of 10 respondents were “very concerned” about security risks related to employee use of mobile and wireless technologies, while 32 percent categorized themselves as “somewhat concerned.” As Figure 1 shows, security risks are the highest barrier to more widespread adoption of mobile and wireless by government, by a large margin (see Figure 1).

Although two-thirds of the survey respondents say they’ve installed mobile device security solutions, they remained extremely concerned about the extent of their protection. In fact, more than a third say they either need to upgrade or will upgrade their security solutions.

The main security concerns cited were robust identity authentication and credential management, potential data loss and leakage, viruses and malware introduced via mobile devices, secure and timely identity provisioning, and the need for more widespread use of data encryption.

“All of these issues have one thing in common: You don’t want people to have access to information that they shouldn’t have access to,” says Josh Sawislak, a senior fellow at the Telework Exchange, a public/private partnership focusing on the federal telework and mobile community. “At the same time, users have to be able to get to the data they need, and without that, these systems are useless. It’s a tough balancing act.”

Balancing act

However, that balancing act is eminently doable, says Chris Smith, U.S. federal chief technology and innovation officer at Accenture

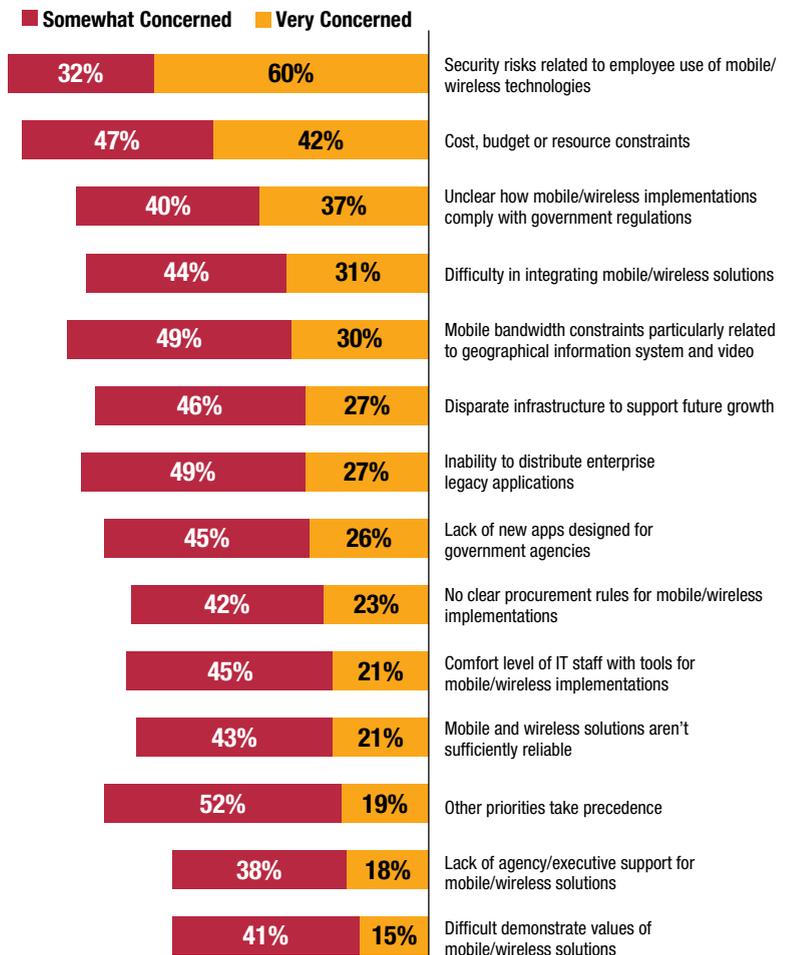
Federal Services and formerly CIO at the U.S. Department of Agriculture.

“Security has to be built into how you architect and execute a solution,” Smith says. “Start with a mobile device management approach, and then architect your applications so they are secure sitting on top of that, and then make sure that they are secure when traversing the network.”

Mobile device management begins with implementing policies and procedures to ensure that sensitive data never actually resides on a mobile device. To help agencies,

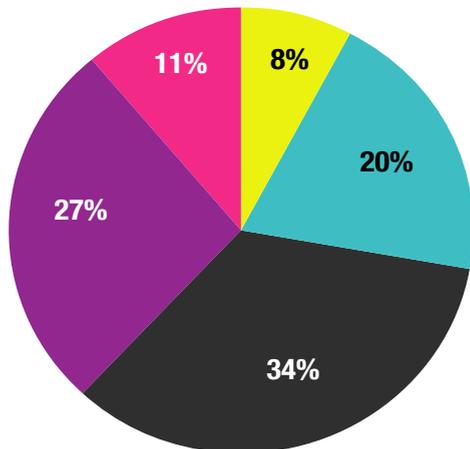
MANY SERIOUS BARRIERS TO INCREASED MOBILE USE

% of respondents who indicated the level of concern about specific obstacles to increased deployment



Few employees comply with mobile device rules?

% of respondents with an opinion about this statement: *Too many of our agency employees don't follow security and data backup procedures with their mobile devices*



■ Strongly Agree
 ■ Neutral
 ■ Disagree Strongly
■ Agree Somewhat
 ■ Disagree Somewhat

the National Institute of Standards and Technology offers a series of guidelines to help agency managers manage mobile devices. With a mobile device management policy in place and mobile device management tools being properly used, if the device is ever compromised, the data won't be compromised as well.

"The ideal situation is where credentialed users can access the information they need on mobile devices but not store the data on those devices," Smith explains. "But if for some reason some information has to be stored on the device,

make sure the encryption on the device is sufficient."

No matter what else you do, be thoughtful about what information and applications can be accessed via mobile device.

"Don't just grab your most highly complex compute problem with a lot of personally identifiable information on it and put it in a mobile app without thinking through your mobile device management strategy, how you are monitoring things on an ongoing basis and controlling those policies," Smith notes.

According to the survey, half of the agency decision-makers say their employees fail to follow proper data backup and security procedures for their mobile devices. Although this problem might be even more acute at state and local government offices, it appears that fewer than 20 percent of respondents don't worry about employee compliance (see Figure 2).

There is a simple fix to that, experts say: mobile device management. This type of off-the-shelf solution addresses just this kind of problem by automating the procedure.

Other barriers

Other concerns cited by study participants include budget and resource constraints, including a lack of confidence that agencies have the resources to manage wireless initiatives; confusion about how mobile/wireless implementations will comply with government regulations; and difficulty in integrating mobile/wireless solutions. As Figure 1 above shows, roughly half of respondents indicated some level of concern about more than 14 different types of concerns.

Those concerns make a great deal of sense, says Sawislak; he says the two biggest barriers to the increased adoption of mobile computing in government are culture and policy.

"It's not as much of a technology issue; the technology is there," Sawislak says. "It's about updating the [Federal Information Security Management Act] rules to reflect

NIST guidelines for securing mobile devices

- Develop system threat models for mobile devices and the resources accessed through them.
- Evaluate the pros and cons of each provided security service, determine which services are needed, and then design and acquire the solutions that provide those services.
- Have a mobile device security policy.
- Implement and test a prototype of your mobile device solution before putting it into production.
- Fully secure each agency-issued mobile device before allowing users to access it.
- Regularly maintain mobile device security.

Source: Guidelines for Managing and Securing Mobile Devices in the Enterprise, NIST, July 2012



mobile and cloud computing, privacy controls, application security and other cybersecurity issues. These changes are critical to truly enabling a mobile workforce.” Industry experts say these changes are due sometime in 2012.

Another troubling barrier is, ironically, the surging popularity of mobile devices. About one-third of survey respondents aren’t certain that they can effectively manage

the explosion of interest in mobile/wireless functionality.

There is only one answer to that, Sawislak says.

“They have no choice. If they don’t find a way, they won’t be able to recruit and retain top people,” he says. “It’s not just about saving money on office space or commuting costs or having a continuity plan. It’s also about retaining valuable government employees.” ●



THE RIGHT TECHNOLOGY TO MAKE A DIFFERENCE

VERIZON HAS THE EXPERIENCE, NETWORK AND STRATEGIC ALLIANCES TO HELP YOU ADVANCE YOUR PROGRAMS.

VERIZON SOLUTIONS FOR GOVERNMENT



LOGISTICS AUTOMATION

ASSET MANAGEMENT

MONITORING & CONTROL

MOBILE OFFICE

MOBILE HEALTH

Verizon technology enables federal government solutions that facilitate the tracking of equipment, supplies and mobile personnel to serve the public in a more efficient manner. Through innovative solutions like Asset Management, Verizon helps ensure critical services and supplies are safely deployed when and where they need to be in a state of emergency. And it's all made possible with the security and reliability of America's largest 4G LTE network.

Start making a difference for your agency.
Visit: verizonwireless.com/government

