

SPECIAL REPORT

# BYOD

BYOD PRESENTS  
BENEFITS,  
CHALLENGES FOR  
MOBILE STRATEGIES

PAGE 2

SECURITY,  
MANAGEMENT  
ISSUES THREATEN  
TO STALL BYOD

PAGE 4

IS BYOD REALLY  
THAT IMPORTANT TO  
MILLENNIALS?

PAGE 6

VIRTUALIZATION,  
ALREADY A MAJOR  
TREND, CAN HELP  
WITH BYOD

PAGE 7

IMPLEMENTING  
BYOD IS NOT EASY,  
BUT HERE ARE WAYS  
TO START

PAGE 9



# BYOD PRESENTS BENEFITS, CHALLENGES FOR MOBILE STRATEGIES

Communications are rapidly going mobile and away from the fixed desktop, and government is heading the same way. One of the most heated debates currently is over bring your own device (BYOD), which promises a dramatic reduction in the costs agencies face to provide the equipment and infrastructure needed to enable their workforces to take advantage of the mobile communications boom. Other advantages, such as significant boosts in employee productivity, are also potential benefits.

The influence of mobile on government operations was recognized in the Obama administration's Digital Government Strategy, published in May 2012. One of its three primary objectives is to "enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device." The understanding that BYOD will play a part in that is evident throughout the strategy document.

In fact, one of the specific deliverables of the strategy is a set of guidelines derived from agency pilots that government overall can use to implement BYOD. A BYOD Toolkit was published in August as a first stab at providing those guidelines. A pilot program at the Agriculture Department was highlighted in the toolkit document, but other government agencies — such as the Defense Department, NASA and the Department of Veterans Affairs — are also looking at their future use of BYOD.

USDA has now gone beyond the pilot program and become one of the first agencies to include BYOD in a procurement. Also in August, it published a request for proposals for a five-year, \$20 million "next generation mobility initiative" that could expand the number of mobile users at the agency from 15,000 to 100,000, using a combination of government-furnished equipment and BYOD policies.

This expectation of the use of BYOD in government is buttressed by the estimates for it globally. Although admitting it presents a "security nightmare," Juniper Research recently projected that the number of enterprise users of their own devices will more than double in the next two years — to 350 million from around 150 million.

A 2011 survey by MeriTalk found that as many as 40 percent of defense and civilian agencies allowed employees limited use of their own devices at work, under various strict policies. On the other hand, a more recent survey by GovLoop, the social network for "government innovators," found that only 20 percent of agencies have policies specifically for BYOD.

For most agencies, BYOD is a tough call because the implications of introducing it broadly are not well understood, and at the moment, the perceived problems far outweigh the advantages. DOD, for example, has launched some 20 pilot projects to see how mobile devices can be used throughout its enterprise but seems far from taking the same kind of BYOD leap that USDA has.

"BYOD currently presents many more challenges than benefits and will not be a viable IT mobility model for the DOD in the near future," said Lt. Col. Damien Pickart, a DOD spokesman. Although BYOD does provide the same mobile services as government-furnished equipment, he said, there are "significant legal, privacy and security challenges that must first be resolved, such as multivendor support, supply chain management, cost sharing, reimbursement models, data ownership, device forensic processes and security controls."

As vendors develop secure solutions, DOD will take advantage of the personal productivity gains offered by BYOD, but only when strict information security controls are present at all layers of the mobile device and enterprise infrastructure, he said.

The National Oceanic and Atmospheric Administration has a highly mobile and dispersed workforce that could definitely benefit from BYOD. However, it, too, is taking a cautious approach to BYOD for the same reasons that DOD is and also because of the potential disruptions it can cause to the agency's operations.

You do need to look at considerations such as mission, cost, acceptable risk and the functionality that can be brought to bear through a BYOD program and how that would support the mission, said Daniel McCrae, director of the Service Delivery Division at NOAA's Office of the CIO.

"The other piece is that, as much as we need to be smart about how we deploy and manage the tools, we need to be smart about how we manage the expectations," he said. "BYOD means different things to different people, and having a common expectation of what that means in the organizational and mission context is important."

You'd have to balance the potential of a BYOD program with the reality of the applications or virtual work space that workers would need to access for their jobs, he said, which means making sure that their devices and systems would support the kind of work space they need to be productive.

There are some parts of the government, such as the intelligence agencies, that might never adopt BYOD because of security concerns that will probably never go away. However, it's becoming evident to many both inside and outside government that the current pressure on agencies to increasingly perform better while dealing with tight budgets will force at least parts of the government to go with BYOD.

"In government, you have customers, partners and employees, and in any one of those audiences, you have a range of different users, such as teleworkers, field agents, inspectors and others," said Owen Unangst, director of enterprise mobile computing at Unisys Federal Systems and a former associate CIO at USDA. "Agencies will not be able to provide all of those people with a government device, so they will be forced to bring in BYOD and then have to come up with a way to manage the devices adequately."

If the government doesn't mind staying a little behind the curve on efficiencies, it will be fine to declare just a small set of devices that users will be authorized to have

and that can be relatively easily managed, he said.

"But that's the dilemma right there because government employees, particularly the mobile elites and leaders in agencies, are starting to say they don't want a device that makes them do things in a less efficient way," he said. "With agencies providing every piece of technology, so constrained as they are by budgets and technical resources, if they keep things in IT where they continue approving everything, they will get further and further behind in delivering up-to-date services to the American public."

VA is certainly one agency that's been focused on customer needs and has already been using BYOD to some degree to enable its staff to do their job of providing services to veterans. Although they are not yet allowed to connect to VA's internal network using their own devices, said Donald Kachman, VA's director of mobile and security assurance, they can access some resources on their personal devices through external connections using VA's remote access tools.

As the technology matures, he said, there should be options to further reduce government devices and increase the number of remote employees who have secure access to VA applications and software resources.

However, Kachman, along with most other government and industry sources, does not see BYOD as a leading force for the transformation in IT and communications that mobile technology is introducing. Ironically, as BYOD management processes improve, they believe the term will eventually disappear.

"I think mobile is transformative," Kachman said. "I think BYOD is a component that not only takes advantage of that transformation but also brings a reduction in costs to the government."

# SECURITY, MANAGEMENT ISSUES THREATEN TO STALL BYOD

There are a myriad of concerns for agencies in adopting bring-your-own-device policies, but it's safe to say that security is near the top of most lists.

To federal IT managers, BYOD can be a nightmare, taking them outside of the tightly-controlled universe of government-furnished equipment — where agencies can closely manage such things as operating system updates, the applications on the device and how data is accessed — to the hodgepodge of operating systems, versions, applications and device hardware that BYOD represents.

In a July 2012 draft update to its guidelines on managing and securing mobile devices (SP 800-124), the National Institute of Standards and Technology (NIST) said that BYOD is a particularly untrustworthy way to introduce mobile devices into the government enterprise.

Current mobile devices lack the technical basis for trust features that are increasingly built into laptops and other kinds of host systems, it said. There are also frequent jailbreaking and rooting of mobile devices, “which means that the built-in restrictions on security, operating system use etc. have been bypassed.”

“Organizations should assume that all phones are untrusted unless the organization has properly secured them before user access and monitors them continuously while in use with enterprise applications or data,” NIST said.

Agencies also have questions about how to handle situations with BYOD that current policies just can't cover. Debora Plunkett, the National Security Agency's information assurance director, told the audience at 1105 Media's Cybersecurity Conference in October 2012 about issues involved with breaches of classified information.

“The procedures for dealing with it are to remove the device and, depending on where the device is in the ecosystem, sometimes you have to destroy the device,”

she said. “Imagine how that would work in BYOD where I'd have to say ‘Oops, I need your phone and you can't have it back?’”

No one has provided all the answers to these security concerns yet, but given its importance to the government, a lot of people are working on it. The BYOD Toolkit published by the Obama Administration as a follow on from the Digital Government Strategy it published earlier in 2012 gives ideas of the broad approaches that can be taken:

- Virtualization: Provide remote access to computing resources so that no data or corporate application processing is stored or conducted on the personal device.

- Walled Garden: Contain data or corporate application processing within secure application on the personal device so that it is segregated from personal data.

- Limited Separation: Allow comingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied.

It's an in-depth discussion that people need to engage in for this, said Kyle Keller, cloud business manager for EMC Federal. The first part of that is to ask whether agency data will be going to the user's device, and if so if they will be allowed to copy that data to the device.

“Most customers I talk to say the desire is to give them access, but to maintain the data in their own or a shared data center they have with other agencies,” he said. “In that case, the question is how to take a data centric approach and secure the data and [control] access to it using two-factor authentication or something else.”

Organizations then need to consider the possibility that devices will be lost or stolen. The ability to remotely wipe a device clean is a “huge factor” in BYOD, he said.

Other approaches to security in the near future could

include such options as implementing a hypervisor on the device itself. This would enable the IT department to create a specific work number for the user, set up a virtual instance of their workspace, and provide containers on the device that would automatically encrypt agency data.

A holistic approach to security would also help with identifying where BYOD makes sense in an organization and where it doesn't, said Daniel McCrae, director of NOAA's service delivery division. Such a managed risk approach would include things like the need for device security, use policies, encryption, remote management and so on.

"If you look at the nature of the work and a risk assessment points to a high degree of risk, or risk mitigation measures that would result in severely limited functionality, then maybe that type of work is not a good BYOD candidate," he said.

So, any evaluation needs to start from the mission requirement said and determine if the nature of the work lends itself to a BYOD environment. That certainly doesn't mean that there would be no security, McCrae said, "but if it's to the point where the benefits are obviated because you do have that severely reduced functionality on the device, then chances are that the things they are trying to do with it are not a good fit for BYOD."

Another essential factor in security is the choice and use of mobile device management (MDM) tools, which provide a way for agency IT managers to centrally manage a range of different mobile devices and operating systems. They would be needed anyway, given the range of mobile devices that agencies will be taking on even if they provide those themselves. But there will be no way to manage and secure BYOD devices without them.

The problem with current MDMs, according to Tom Simmons, vice president of the U.S. Public sector for Citrix Systems, is that they generally require employees to provide rights to agencies so that they can manage device-based data and get access to the device-based components of the MDM technology. And as NSA's Plunkett pointed out, they also would have to grant the government permission to use the MDM to wipe that device if it were compromised or lost.

"What we're finding is that a lot of union negotiations and employee preferences would preclude the MDM of today from being the solution for BYOD," he said.

What that is leading to in the near future are families of management solutions that embrace such things as mobile application management (MAM), mobile operations management (MOM) and other scenarios.

"In that case, it's less dependent on putting a management technology on the device and more about managing the user profile and the applications and data that the user would have access to from any particular device," Simmons said.

MDM was a decent descriptor a few years ago "when you were talking about a set of APIs to turn Bluetooth on or wireless off or to wipe the entire device," said Chris Roberts, vice president, public sector for Good Technology. "Now, it's got to become more of an enterprise mobility solution, a comprehensive platform to cover all of the relevant areas."

That will be essential going forward, he said. Users are comfortable with government wiping a set of government apps and data from a device, but they don't want their personal apps or data to be touched.

"This is where BYOD is stalling out right now, when end users look at the policies they are being asked to sign," Roberts said. "So, if government just sticks with device management alone, then my prediction is that the adoption of BYOD will be slow going."

# IS BYOD REALLY THAT IMPORTANT TO MILLENNIALS?

There are a number of advantages claimed for a bring-your-own-device (BYOD) environment, and the reduction in the costs of procuring devices and then paying for their use is just one. Another is the need to attract and keep the newer generation of workers, who are adept at using mobile devices and expect the services they provide to be available to them in the workplace.

Is that true? As with most things in this “digital native” argument, it depends on whom you ask. Jeremy Sherwood, product manager of virtualization and cloud at ScienceLogic, for example, believes there is “absolutely some huge validity” to this demographic argument.

“Because younger people grow up with the devices and constantly use them, they are accustomed to them being available and expect to be able to leverage the devices and the offerings that are made through them,” he said. “It’s not the devices themselves so much but that the apps they use are in the cloud, and it’s more their choice as to whether they use them for [the work] they have to do.”

Agency managers also readily recognize the potential. Daniel McCrae, director of the Service Delivery Division at the National Oceanic and Atmospheric Administration’s Office of the CIO, said NOAA can “certainly take advantage of employees walking through the door [who are] familiar with the computing platform they are going to be using.”

“It’s clear that millennials and younger employees probably do feel more comfortable with the kinds of things BYOD offers,” he added, “and in many ways will expect them.”

GovLoop, the social network for “government innovators,” recently surveyed its members about BYOD issues. Of the responses provided by the survey, “allowing people to work on the most comfortable device” was the greatest benefit of BYOD (71 percent agreed), followed by improved productivity (58 percent). Nearly 80 percent of respondents added employee satisfaction, engagement and

productivity as a positive impact.

Kimberly Hancher, CIO at the Equal Employment Opportunity Commission, one of the earliest adopters of BYOD in the federal government, was quoted in the report as saying that, from an employee standpoint, smart phones and tablets have become an extension of an individual’s personality and personal productivity.

“One of the benefits [of BYOD] is that if a person is very proficient on a device, they should take that proficiency into the workplace rather than learning how to be minimally proficient with the government-provided device,” she said. “I can’t overemphasize how important personal productivity is across the enterprise.”

On the other hand, only a little more than half of the people surveyed by GovLoop believed BYOD could serve as a retention and recruitment tool, though millennials and teleworkers were those who most believed it would be.

Pat Fiorenza, a research analyst at GovLoop and a principal author of the survey report, said in an interview that he thinks the generational split in the use of mobile devices is “often over-generalized.”

“I do think that millennials have a different perspective of what resources should be available and where the attention should be placed,” he said. “But I think all generations have things they do with these new technologies.”

Overall, Fiorenza said, BYOD is just one part of the overall IT trends in government, though it’s one that falls into the critical area of collaboration and speaks to how agencies will open up access and communication channels to enable that.

“So, for me, this is a silver lining about how government is thinking about how to engage with major stakeholders,” he said. “It’s a key for the whole area of data movement and how to use information and knowledge for better decision-making.”

# VIRTUALIZATION, ALREADY A MAJOR TREND, CAN HELP WITH BYOD

A range of technologies are enablers for a bring-your-own-device environment, but arguably none is as important as virtualization. The good news for government organizations is that, because it's something most of them are grappling with now through server consolidation and virtual desktop initiatives, BYOD could be a relatively easy fit.

It's something that Daniel McCrae, director of the Service Delivery Division at the National Oceanic and Atmospheric Administration's Office of the CIO, sees as a necessity for NOAA. He pointed to the highly mobile and dispersed workers that the agency employs to track the weather and what BYOD would mean for them. The biggest challenge will be replicating the virtual work space of those workers and bringing that to the BYOD environment.

"Virtualization in general is really critical to the way we will carry out the mission in the future because that's where you really begin to leverage some of the advantages of IT, whether it's on traditional desktop computing, notebooks or other mobile platforms," he said. "Being able to virtualize your work space and then deliver that is when you can really start to see the major improvements in productivity."

One of the case studies included as an example in the Obama administration's BYOD Toolkit is that of the Alcohol and Tobacco Tax and Trade Bureau, which, like NOAA, has a widely dispersed workforce with many people working from home full time. More than 80 percent of its workforce regularly teleworks.

The bureau spent about \$2 million every four years or so to refresh the desktop and laptop computers for its workers, with the added cost of the several months of disruption that caused to the organization's IT program and business users. To get around this, officials decided to go with a virtual desktop solution that centralized all

the computing power, data and applications, and simply allow users to access them through a thin client.

It saved the bureau \$1.2 million, more than paying for the virtual desktop implementation. It also laid the foundations for the agency's eventual introduction of BYOD.

"Because no data touches the BYOD device and no work is physically accomplished on the BYOD equipment," according to the case study report, "all requests for discovery of information from a user's computer can be satisfied without having to recover anything from the user's device."

Virtualization also centralizes the security and access policies an organization develops for all its IT users, said Jeremy Sherwood, product manager of virtualization and cloud at ScienceLogic. That mitigates the risk across the board because if the server, desktop and BYOD interactions are all virtualized, "this builds a nice, pretty umbrella of security around all of these assets."

"They are all in the same place and under the same set of rules," he said, "and then the systems interfacing with them are irrelevant because the security controls are a part of the virtualized infrastructure."

The process of virtualization, which most agencies are involved with, makes BYOD "an easy plug-and-play," he said.

It also makes the cloud a potentially important enabler for BYOD, though it's not a critical must-have, said Tom Simmons, area vice president for the U.S. public sector at Citrix Systems.

"There are technologies today where I can authenticate and gain access to the infrastructure needed for the virtual work space," he said. "The savings and flexibility of hosting that virtual work space or virtual app in the cloud [are] more of a cost component in considering the cloud and so [are] more of an option

than necessity for BYOD.”

So it comes down to what solution fits best. The cloud is there if agencies feel the need to cut costs even more, but there are technologies widely available on the market today that can deliver a similar service, with all the relevant security controls, directly from an agency’s own data center.

# IMPLEMENTING BYOD IS NOT EASY, BUT HERE ARE WAYS TO START

As early as it is in the government's consideration of bring-your-own-device policies, one thing that's already evident is that implementing BYOD won't be a simple process for agencies. In some respects, the technical part will be the easiest.

The Obama administration outlined the problems agencies face in its recently published BYOD Toolkit:

"Implementation of a BYOD program presents agencies with a myriad of security, policy, technical, and legal challenges not only to internal communications, but also to relationships and trust with business and government partners. The magnitude of the issues is a function of both the sensitivity of the underlying data and the amount of processing and data storage allowed on the personal device based on the technical approach adopted."

It would also be a mistake for agencies to go into this believing that BYOD has to apply to everything that employees do, said Donald Kachman, director of mobile and security assurance at the Department of Veterans Affairs. BYOD might turn out to provide a system more comfortable to users for their specific jobs, and that could require policy and cultural changes.

Additionally, he said, employees will have to be educated across the government about what BYOD requires.

"The fact is that many individuals do not even set a simple password on their personal mobile devices, even though they have many apps that contain a large portion of their lives," he said. "Connecting to unknown networks, downloading apps that may be malicious, etc., are all things that must get all federal employees' attention."

GovLoop, in a report following its survey of government "digital innovators," came out with five steps it believes agencies can take to smooth the path to BYOD:

1) Meet with key stakeholders to develop a pilot plan. At the onset of developing a BYOD policy, agency

leaders should sit down with key stakeholders within the agency to discuss what a BYOD initiative looks like. Staff members from all functional areas should be present to provide input and feedback. This will also help develop buy-in and create a unified vision for the agency's BYOD program.

2) Meet with the legal team. BYOD is new in government, and there is a lack of legal precedent. So be sure to meet with legal advisers to mitigate legal risks.

3) Craft an internal policy for BYOD. After you have met with key stakeholders and the agency's legal team, begin to craft the BYOD policy. Be sure to incorporate feedback from the legal team and agency leaders.

4) Announce the program to employees. As with any program, announcing and selling it to employees is critical. If it is a pilot program, be careful how you select employees and develop a team.

5) Iterate, review outcomes and improve the BYOD strategy. Once the program has been initiated, be sure to set up periodic checkpoints with end users and administrators so they can provide feedback on the program.

There is no single fount of BYOD best practices, but there are some sources with suggestions about what to use when forming BYOD policies. GovLoop's report has many, and the National Institute of Standards and Technology's current revision of SP 800-124 gives general guidance on how to accommodate BYOD in the context of an overall approach to mobile devices.

The BYOD Toolkit also provides five examples of BYOD policies that agencies could use in forming their own:

- Policy and Guidelines for Government-Provided Mobile Device Usage
- BYOD Policy and Rules of Behavior
- Mobile Information Technology Device Policy
- Wireless Communication Reimbursement Program
- Portable Wireless Network Access Device Policy •