A Forrester Consulting Thought Leadership Paper Commissioned By Cisco Systems

BYOD In Government: Prepare For The Rising Tide

October 2012

FORRESTER®

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

Table Of Contents

About Forrester Consulting
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.

Executive Summary

Forrester's study of the use of personal devices for work purposes within government organizations yielded the following key findings:

- **Government employees use personal devices for work purposes . . .** A survey that Forrester Consulting conducted on behalf of Cisco found that 58% of information workers in government that use a smartphone for work purposes purchased that device without considering what the organization supports. Government IT decision-makers must face the reality that employees are bringing their own devices to work.
- **. . .yet bring-your-own-device (BYOD) policies, when they exist at all, are nascent.** Few organizations have their head in the sand about the reality of BYOD. But most are still in the research and pilot stages and have conducted limited trials of device subsidies, policy-based application access, and mobile device management. Few if any government organizations have agencywide BYOD programs; according to the survey, only 6% of those using personal smartphones and 4% of those using personal mobile phones received a subsidy.
- **Security concerns impede the rollout of BYOD policies for many organizations.** The biggest worry among government IT decision-makers is the security of applications and the data they contain. They ask: How do we secure the device, the applications, and the data? How do we ensure that information isn't transferred to insecure locations?
- **BYOD implications extend beyond IT to human resources (HR) and legal concerns.** The concerns of IT leaders don't stop with technology. Liability is a major concern: Who is liable in case a device is lost or stolen? HR implications are another concern: The use of personal devices blurs the dividing line between work and personal life and violates the strict working conditions that public-sector unions impose in some countries.
- **CIOs craft BYOD strategies to enable productivity while protecting application and data security.** Government IT decision-makers recognize the inevitability of BYOD and set out to define their terms. But the BYOD trend has raised additional questions around the workforce and the workplace of the future — a broader spectrum of issues that government organizations will have to address.

Government Employees Use Personal Devices For Work Purposes

The use of personal devices for work purposes is generally considered inevitable across all industries — and that includes government employees.[1] Although government organizations have not typically been known as hotbeds of technology, their retro status is changing as employees bring their own devices to work. Some early-adopting public-sector organizations already provide device choice; employees select the device they need from a catalog of authorized devices and services. But even those organizations that embrace flexibility and choice are being pushed by the demand for the use of personal devices. For example, if a particular smartphone or tablet is not in the catalog, employees request permission to use their own.

"BYOD is an inevitable outcome. The challenge is how you manage the transition." (CIO, UK county council)

Forrester Consulting's survey of government employees indicates that this trend is prevalent across government organizations:

- **Government organizations issue mobile phones and laptops to employees . . .** 62% of government information workers are issued laptops with no choice of make or model; for mobile phones, 50% are issued a standard device (see Figure 1). Typically, government organizations typically pay for standard-issue devices (see Figure 2).

- **. . . but most government employees use smartphones and tablets they've purchased themselves.** According to the survey, 58% of information workers in government that use a smartphone for work purposes purchased that device without considering what the organization supports. And 48% of those that use tablets purchased their own without considering what their employer supports. And they pay for the devices themselves: 59% of smartphone users and 47% of tablet users reported that they paid for their own devices. Employees are often filling gaps with devices they purchase themselves. As a desktop services director at a provincial government department in Canada noted, "We see more demand for tablets because we don't offer them right now."

- **Device choice through a service catalog and shared device costs are less common.** Some government organizations do provide a choice of devices: 25% of tablet users and 16% of smartphone users purchased their devices from a list of authorized devices. Purchases from these service catalogs are most common for ultraportable laptops.

- **Elected leaders, senior management, and mobile workers drive demand . . .** Generally, the demand to use personal devices comes from those who need to be mobile and contactable: managers in meetings, case workers out in the field, and after-hours tech support. But we heard that senior management and elected officials also push to use their personal devices — and pressure from managers and elected officials often carries more weight.

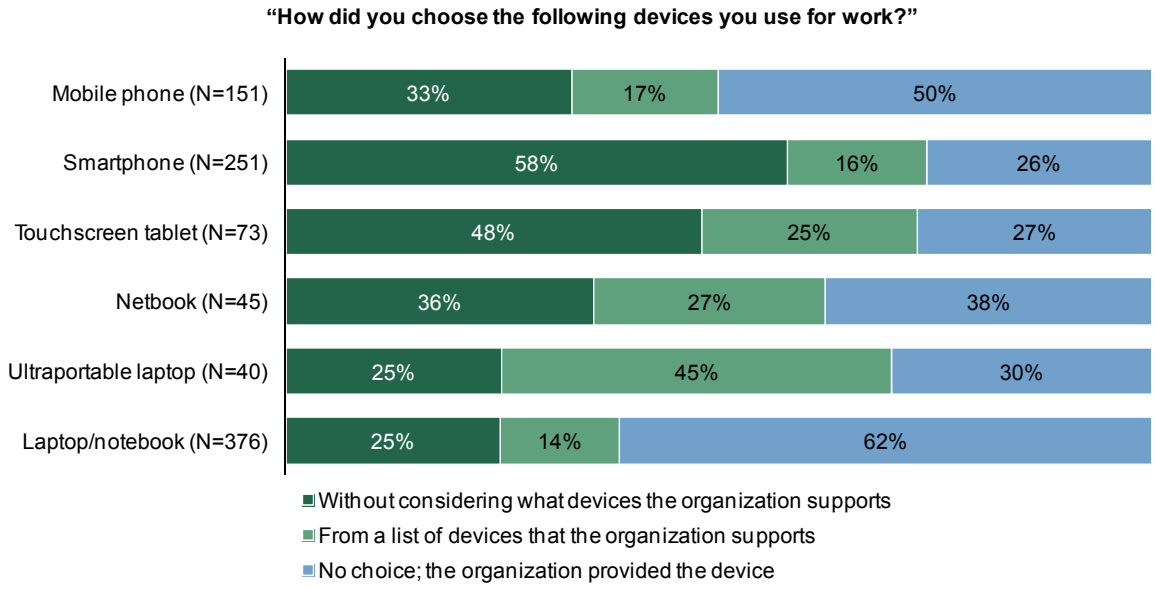
- **. . . primarily to check email and calendar appointments . . .** Government executives and information workers want to keep up on email and urgent communications when traveling or out of the office. But increasingly, employees used to reading personal email on a smartphone also want access to their work email on their personal device in order to check in on their own time.

"Email and a few business applications top the list of use cases. Executives are looking to catch up on email and urgent communications when traveling. They are also using these devices to read and update documents such as proposals and presentations." (Deputy director, UK central government organization)

- **. . . with some demand for access to line-of-business apps and data.** Demand for access to applications and data varies widely across organizations. Local governments see the need for more flexible access to CRM or case management software, whereas social services employees find it useful to manage cases from personal devices while on site. Some research organizations collaborate with external international organizations whose researchers need access to internal data on their personal devices.

- **Mobile access on either cellular or Wi-Fi networks dominates.** Most IT decision-makers surveyed anticipate a greater use of personal devices through mobile access. A select few employees, such as heavy graphics users or application developers, may request the use of a specific device in their office. But the vast majority of government employees using personal devices for work do so via mobile access.

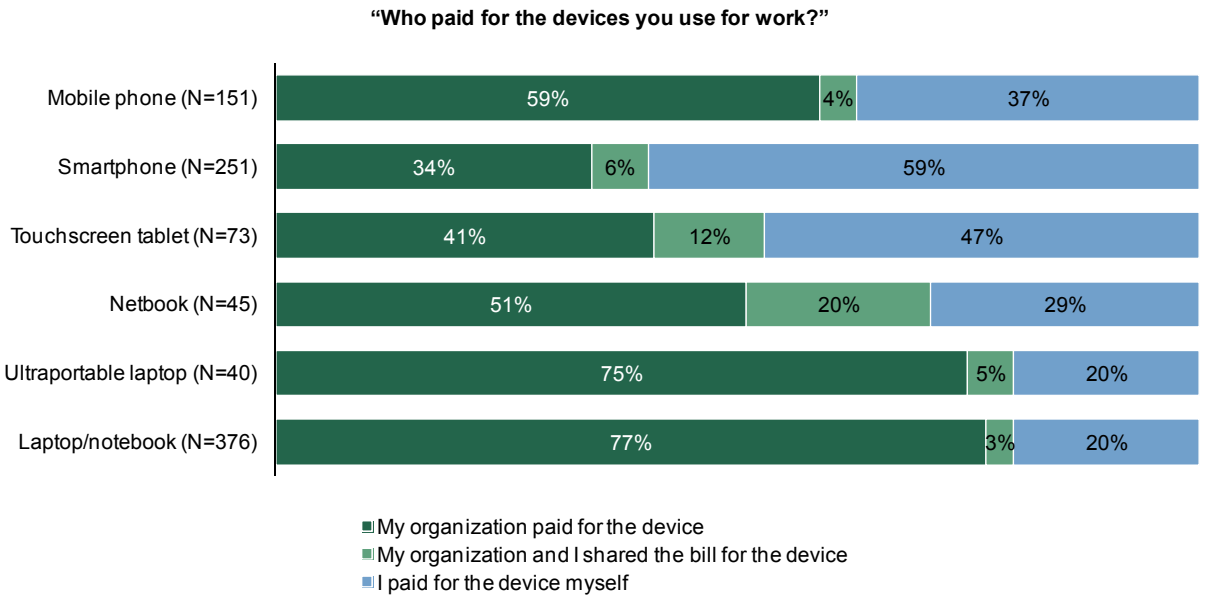
Figure 1
The Majority Of Government Employees Independently Choose The Smartphones They Use For Work Purposes



Base: Information workers from government agencies worldwide who use a mobile device for work

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Figure 2
It's All Or Nothing: Few Government Employees Receive Subsidies For Device Purchases



Base: Information workers from government agencies worldwide who use a mobile device for work

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Employee Benefits Drive Personal Device Usage; The Savings Are Less Clear

Employees — and the benefits they expect — are driving the use of personal devices in government organizations.

- **Personal devices are mainly being used today for convenience . . .** For many employees, including most government employees, consolidating work and personal use into a single device eliminates the need to juggle multiple devices. According to an IT decision-maker at a local government council in the UK, even those employees who weren't originally perceived to be mobile workers and didn't have a council-issued device began to use their personal devices because they reasoned that "If I could, wouldn't that be better?"

"Even when someone may not need a tablet or smartphone to do their day-to-day work, having one may help manage life better. Moreover, new employees who have used a smartphone or tablet elsewhere — either in a former job, at school, or at home — expect to maintain the convenience to which they've become accustomed." (Head of IT, Canadian municipal agency)

"Organizations usually try to make the business case for BYOD around reducing paper — but in reality it's a convenience thing." (CIO, local government)

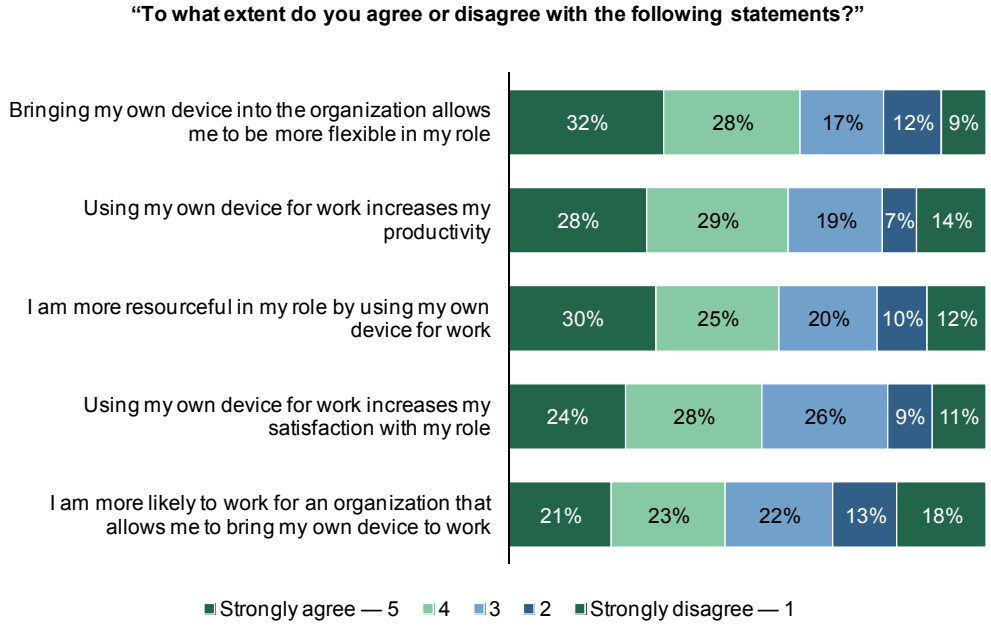
- **. . . and carry expectations of increased flexibility, productivity, and resourcefulness.** According to the current study, 60% of respondents reported that bringing their own device into the organization allows them to be more productive in their role; 57% believe that using their own device makes them more productive; and 55% believe that they are more resourceful if they're able to use their own device (see Figure 3).

- **Personal device use increases job satisfaction but doesn't always influence job choice — yet.** Of government information workers who use mobile devices for work, 52% reported increased job satisfaction as a result. That figure is expected to grow, as is the 44% who reported that the ability to use a personal device will positively influence job choice.

"Demographic changes in the coming years mean that potential employees will be swayed by technology and how forward-thinking an employer is in terms of what is allowed and not allowed. The perception of flexibility and forward-thinking will be critical to finding talented staff." (Director of IT, national health organization)

"Try to resist and you will see what it does to satisfaction!" (Head of IT, UK county council)

Figure 3
Employees See BYOD As Increasing Their Flexibility, Productivity, And Resourcefulness



Base: 498 information workers from government agencies worldwide who use a mobile device for work
("Don't know" responses have been omitted)

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

- **Most government CIOs don't have a clear picture of the ROI or cost advantages of BYOD.** Cost benefits depend on device acquisition policies. In one US state, the government's adoption of a new policy to allow the use of personal devices led to an 18% to 20% reduction in government-issued devices. That's cost savings. But several CIOs surveyed believe that the key cost-saving potential lies in day-to-day support. For example, the director of corporate IT at a national health organization told us: "We don't have to provide the same level of support for BYOD — people are now responsible for their own devices." The perception that support costs will be lower, however, has not been tested.

"It would be an exercise in justifying to our policymakers that there's a cost benefit in driving down the use of state-owned equipment by allowing employees to use and manage their own devices. Cost/benefit analyses are more straightforward at enterprises; it just doesn't work the same way in state government." (IT director, US state government)

But a comprehensive IT strategy including BYOD and improved security can reduce costs:

"The consumer approach would dramatically reduce costs. We calculated that running consumer devices and providing a shared desktop for line-of-business apps is 20% of the cost of running standard locked-down devices — and the experience is 100 times better. We saved about 81% in IT costs. On an individual level, we save about £1,200 per year, because comparatives are expensive — restricted device costs were £1,600 a year for a locked-down laptop and support services on the OS." (Director Strategic Change, UK cabinet office)

Despite Benefits, BYOD Strategies And Governance Policies Remain Scarce

Few organizations prohibit the use of personal devices outright: Just 6% of government employees surveyed reported that their organization prohibits the use of personal devices. But the majority provides limited or no support: 37% of these organizations provide no support, while 36% provide some support —either full support for selected devices or limited support for all devices (see Figure 4). Just 8% reported that their organization supports all personal devices. And although only 8% of government employees report that their organization does not have an official policy for work-related use of a personal device, those policies are not yet well-defined and in most cases are still works in progress.

"We are headed in the direction of BYOD, but we are taking a very cautious approach." (IT policy advisor, Canadian provincial government)

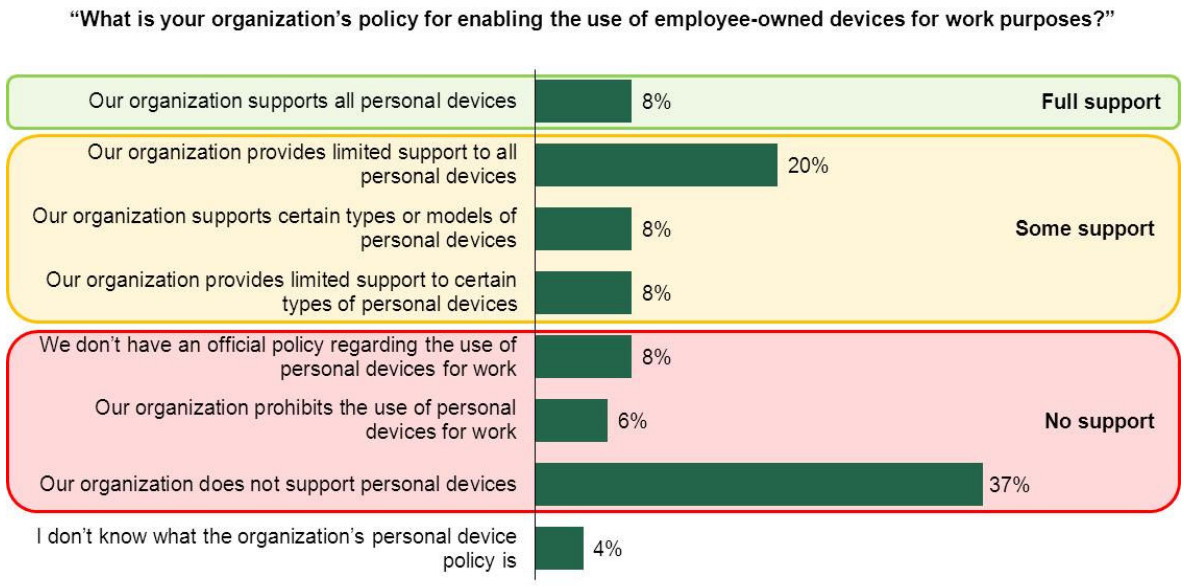
CIOs and IT managers at government organizations report that:

- **Government organizations remain at the research and planning stages with regard to BYOD.** Of the 11 government organizations interviewed, not one in North America had a formal policy governing the use of personal devices. Several had appointed staff members to develop strategy and formulate a policy, but most were in the early days of research and planning. In general, organizations in the UK were much farther along. One exception was a UK county council; while it doesn't call its policy "BYOD," it has a comprehensive "mobile and flex" policy that includes thin-client architecture, two-factor authentication for

applications, and guidelines for personal responsibility. Another national UK organization which openly allows informal use of personal devices plans to roll out its formal policy within six months.

- **Draft policies vary widely across government organizations; device subsidy is a sticky issue.** Some organizations are well down the path of drafting policies with pilot programs targeting specific provisions: one organization in the US federal government is conducting 35 separate pilots to evaluate program alternatives. At the other extreme, one provincial government in Canada reported that they would start to explore more hands on in the next year. One policy element that is difficult to nail down is just how much the device subsidy should be — and how often employees should be eligible for it. But others don't even bother. A university in the southern US indicated that it was including the requirement that applicants provide their own device — typically a smartphone — for the job in its official job descriptions.
- **But delays in centralized BYOD strategies and guidelines can lead to policy proliferation.** Some organizations were concerned about a proliferation of incompatible policies. Several central IT departments included in this study feared that smaller, more nimble agencies within their larger organization were ahead of the curve. One of these told us that these smaller agencies "can be off and running in a short period of time and don't think about a larger policy, whereas the central IT department is looking at it more holistically — and more slowly." In these cases, consolidating and rationalizing competing policies could be tough.

Figure 4
Few Organizations Prohibit The Use Of Personal Devices, But The Majority Provides Limited Or No Support



498 information workers from government agencies worldwide who use a mobile device for work
(percentages do not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, June 2012

Security Concerns Top The Impediments To A Formal Policy Rollout

For most IT decision-makers, the biggest impediments to the use of personal devices in government organizations are the security implications. Government data security and citizen privacy issues are top concerns.

"Security is the reason we don't currently have a policy — ensuring the security of state information and applications and protecting the information of individuals. Privacy and security concerns have slowed the process." (CIO, US state government)

- **BYOD would bring a proliferation of device types and operating systems . . .** Currently, organizations are able to control their IT environment. Many lock down device and operating system options. Organizations fear that they don't have the expertise to secure a more diverse environment, and IT views personal devices as untrusted.

- **. . . and greater temptation for employees to bypass security rules.** It seems that the lack of trust doesn't end with the device. Many organizations are concerned with employees "browsing up" — i.e., looking at information that is more sensitive than they are authorized to view. The reaction is to limit any form of BYOD to people who do not access any protected or restricted information. Other organizations worry about increased use of the cloud. They envision employees uploading information or saving documents to public clouds for access via a personal device — and the popularity of consumer cloud storage suggests that this concern is not unfounded. The use of public clouds also brings concerns about jurisdiction and cross-country data flow, especially data stored in US territory.

- **CIOs investigate device management with emphasis on sandboxing government applications and data.** As personal devices are increasingly used for government work and government-issued devices are used for personal purposes, IT decision-makers worry about the blurring of information ownership and liability.[2] IT organizations are exploring mechanisms to partition or sandbox the data and applications associated with each use. Many organizations are currently investigating — and, in some cases, piloting — the currently available solutions.

- **Others explore new security architectures with protection at the application and data level.** Some organizations envision implementing a security architecture that implements controls on an application-by-application basis. This allows secure applications to sit alongside applications that are wide open without having to protect the device.

"In the long term, we don't want to protect endpoints, and we won't have firewalls. Security will be built into the data and applications. We should be able to accomplish the vast majority of this by changing the security architecture." (CIO, US federal government research agency)

- **Network security and capacity remain an open question.** Most IT decision-makers interviewed were less concerned about network security or capacity. Some focus on security at the application and data layer in order to establish more granular controls; others provide access to the internal wireless network for a personal device through guest wireless access. "Guests" are able to view email and calendars and look up things on the Internet but cannot change data or configurations. Most are still making decisions about wireless and networking, recognizing that capacity increases will be necessary to accommodate increased traffic.

- **Although not top of mind, device diversity will exacerbate application integration challenges.** Few of the CIOs that Forrester Consulting interviewed have spent much time thinking about how BYOD affects application integration and development. However, the use of personal devices will dramatically increase the number of integration scenarios. For example, enabling business applications for mobile devices used to focus on standardized corporate devices. Now, the varieties of employee-owned devices require multiple mobile integration implementations.[3]

The Implications Extend Beyond IT: Political, Legal, And HR Concerns Often Dominate

The use of personal devices by government workers raises issues that extend beyond technology. IT decision-makers are concerned about the political, legal, and HR implications of a formal policy.

> *"We're not concerned about the technology; we're concerned about the HR and legal requirements and implications. If a mobile device is compromised, we worry about how well we have partitioned the device and what government controls we have put on it. Who is responsible for compromised devices?"* (CTO, US federal government research agency)

According to those interviewed, the use of personal devices and the formal policies governing their use:

- **Challenge the classic model of a 9-to-5 government worker; some public-sector unions object.** As several CIOs mentioned, government organizations are often staffed by public-sector union members. In their collective bargaining agreements, there are rules as to how many hours a day employees can work. Unions often do not support BYOD programs because they feel that it is a way for the organization to make employees work more.

- **Raise concerns among government leadership about public perception.** Government organizations already face scrutiny from oversight committees and their constituents over the use of technology, and their leaders worry about public perceptions of BYOD. As one CIO noted, "There was a lot of attention by our legislature in the past for cell phone use. Should civil servants be running around with the latest and greatest technology, especially in times of austerity?"

- **Complicate government compensation and expense reimbursement policies.** In addition to the questions of how much and how often, several CIOs mentioned concerns about the implications of device subsidies or reimbursements on compensation. If employees receive a stipend every few years, is that considered income and would it be taxed accordingly? What happens if an employee leaves after receiving the stipend or before the end of a smartphone contract? Do they pay it back? Who's responsible for the remaining contract or cancellation fees? For many agencies, these remain open questions.

- **Muddy the distinction between personal and work-related information and device responsibility.** If a mobile device is compromised, sandboxing or partitioning comes into play. What if personal information is lost or compromised? Who is ultimately responsible for the device — including replacing it? These questions continue to plague government leaders.

If It's Really Inevitable, How Do You Get There?

The use of personal devices for work purposes is increasing, even in government organizations. It is widely accepted that, over time, new employees will request permission to use the devices they know. However, the collective research by IT decision-makers in government provides a valuable starting point for embarking on the journey toward BYOD.

> *"We know BYOD is coming and we are setting the stage for it. As new people come into the government — the new generation — they are used to a new way of working. We try to position ourselves as an organization that is an attractive employer."* (IT policy advisor, Canadian provincial government)

Here are some observations on how best to set the stage:

- **The process is evolutionary, not revolutionary.** There will be no big bang, regardless of whether the IT environment is tightly controlled or more open. Organizations can't force every employee to bring their own device, but neither can they resist the trend completely. The process will evolve over time, perhaps workgroup by workgroup. Expect to see processes similar to those implemented during the shift to personal computers and the move from desktops to laptops.
- **Policy must not wait; guidelines must be incremental and compatible, and the process collaborative.** As central IT organizations research options and craft comprehensive strategies and policies, lower-level agencies begin to do their own thing. Smaller agencies can react much faster and end up ahead of the curve. Policy proliferation then makes consolidation and rationalization across agencies difficult. If this is the case, it may take a legislative or executive act to make that happen — but that's a scenario best avoided.
- **Ultimately, policy guidelines must be comprehensive but can evolve over time.** The most prepared organizations are those which have already embraced flexible work environments with mobile devices and thin-client architectures accessible from government or home offices. Security mechanisms to support remote access set the stage for the use of personal devices. Device management software that forces sandboxing or segmentation for business and personal use provides the next step. And a granular application and data security policy ensures appropriate access to government information.
- **Couple BYOD with a community-based support model.** Most government organizations are looking to keep management of BYOD programs in-house in the first instance. That said, many organizations are concerned about their own limited resources and lack of capabilities and expertise. IT departments fear the thought of supporting the entire universe of possible devices. However, several have embraced the "friend down the corridor" approach, which encourages end users to help each other — a community support model. Renegade users of unsupported operating systems have traditionally resorted to this approach. Online forums and colleagues can offload support and training needs.
- **Leverage existing resources to inform strategy and policy.** The US federal government's recently launched Bring-Your-Own-Device Toolkit is a product of the Digital Services Advisory Group and Federal Chief Information Officers Council and is designed to support federal agencies implementing BYOD programs. The toolkit provides guidelines for developing policy and case studies of early adopter agencies.[4] The

National Association of State CIOs teamed with a mobility solution provider to develop a BYOD best practices guide to help state governments develop their BYOD strategy and policy.

KEY RECOMMENDATION: USE BYOD TO PREPARE FOR THE WORKPLACE OF THE FUTURE

While the initial push is toward greater mobility, government IT leaders can use the demand for personal devices as a catalyst to review the broader work environment. A flexible work environment doesn't stop with the choice of device, but includes the modes of collaboration and tools to support the way that employees prefer to work with partners, suppliers, constituents, and each other. And that environment isn't limited to technology; preparing for the workplace of the future requires broader thinking about how best to organize workspaces and even real estate assets. The workplace is changing, and employees' demands to be able to use their personal devices is merely the first step.

Appendix A: Methodology

Forrester conducted an online survey of 498 government workers across Australia, Brazil, Canada, China, Germany, India, Japan, Mexico, Saudi Arabia, South Africa, South Korea, the UAE, the UK, and the US to evaluate the demand for BYOD initiatives among public-sector workers. Questions provided to the survey participants asked about how they choose their devices for work, if their organization enables the use of their personal devices for work, and what benefits they have realized from using personal devices for work.

The online survey was followed by interviews with 11 public-sector CIOs asking them about the current state of BYOD in their organizations, the pain points associated with enabling BYOD, and the benefits realized to date from BYOD investments. The study was completed in September 2012.

Appendix B: Endnotes

[1] According to the Forrsights Workforce Employee Survey, Q4 2011, 43% of employees bring their own devices for work purposes. Source: "Charting The Rising Tide Of Bring-Your-Own Technology," Forrester Research, Inc., June 12, 2012.

[2] Right now, the ownership of corporate information on an employee's personal device is murky from a legal perspective. Suppose that an employee has a personal device that he paid for but it links to corporate email. Then imagine that the employee loses it, so the company wipes the device, and in the process deletes valuable personal information. Ultimately, this type of unilateral action by IT will be the basis for a landmark court case to determine data ownership and liability. Source: "Charting The Rising Tide Of Bring-Your-Own Technology," Forrester Research, Inc., June 12, 2012.

[3] Source: "Charting The Rising Tide Of Bring-Your-Own Technology," Forrester Research, Inc., June 12, 2012.

[4] Source: The White House (http://www.whitehouse.gov/digitalgov/bring-your-own-device).