IntelliDyne
EXPERIENCE ABOVE & BEYOND

WHITE PAPER:

STRATEGIC IMPACT PILLARS FOR DEPLOYING EFFECTIVE GOVERNMENT MOBILE COMPUTING APPLICATIONS

IntelliDyne, LLC
February 2012

STRATEGIC IMPACT PILLARS IN DEPLOYING EFFECTIVE GOVERNMENT MOBILE COMPUTING APPLICATIONS

Executive Summary

Mobile computing has become a ubiquitous reality in our interconnected world, and many companies and agencies want to "go mobile" with their employees or with their customers. Mobile device use has been trending upwards since 2003 when the Blackberry was released. A 2011 study by the Pew Research Center found that 35% of the American adults surveyed owned some type of smart phone, and that 25% of owners use their smartphone as their primary Internet access point.[1] By 2014, 90% of organizations will support corporate applications on personal devices.[2] In addition to cell phone use, American adults are also increasingly using wireless networks to connect to the Internet, as illustrated in this chart by the Pew Research Center[3](Figure 1).

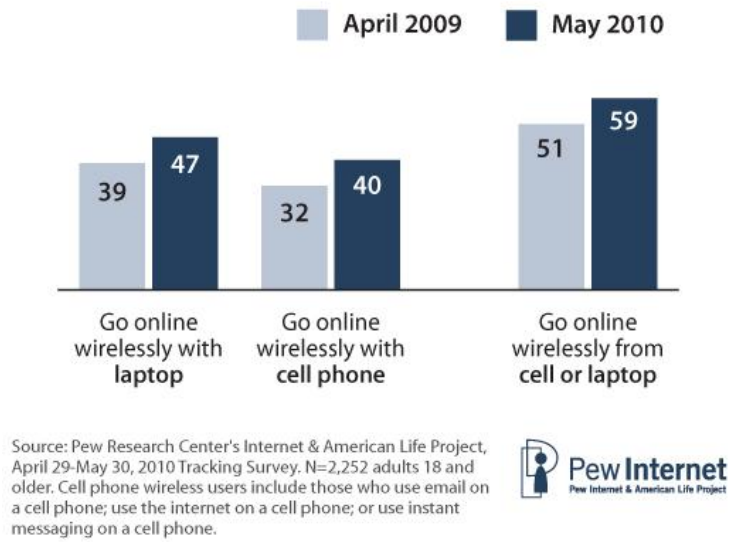

Figure 1: American adults are increasingly using wireless networks to connect to the Internet.

Government IT departments are already seeing the potential in supporting mobile computing within their agencies. At the 2012 Consumer Electronics Show, current Federal CIO Steven VanRoekel announced the creation of new initiatives to change the way the Federal Government integrates and uses mobile

[1] "Smartphone Adoption and Usage," July 11, 2011, http://pewinternet.org/Reports/2011/Smartphones.aspx
[2] "Gartner Top Predictions for 2011: IT's Growing Transparency and Consumerization"
[3] "Mobile Access 2010 Part One: The current state of wireless internet use," July 7, 2010, http://www.pewinternet.com/Reports/2010/Mobile-Access-2010/Part-1/The-current-state-of-wireless-internet-use.aspx?r=1

technology.[4] VanRoeckel acknowledged that "federal agencies have lagged behind the private sector in wireless technology, owing to a constellation of factors including a glacial procurement and in-house development process and an IT culture that has been slow to warm up to many of the new technologies and computing models that private-sector CIOs have already embraced."

However, despite this trend towards mobile computing, it is critical to understand "why" you want to go mobile, and generate a cohesive strategy to create mobile portals and applications, to ensure the security of mobile data, and to centrally manage mobile resources. This white paper outlines four strategic pillars of a mobile computing approach for government IT applications.

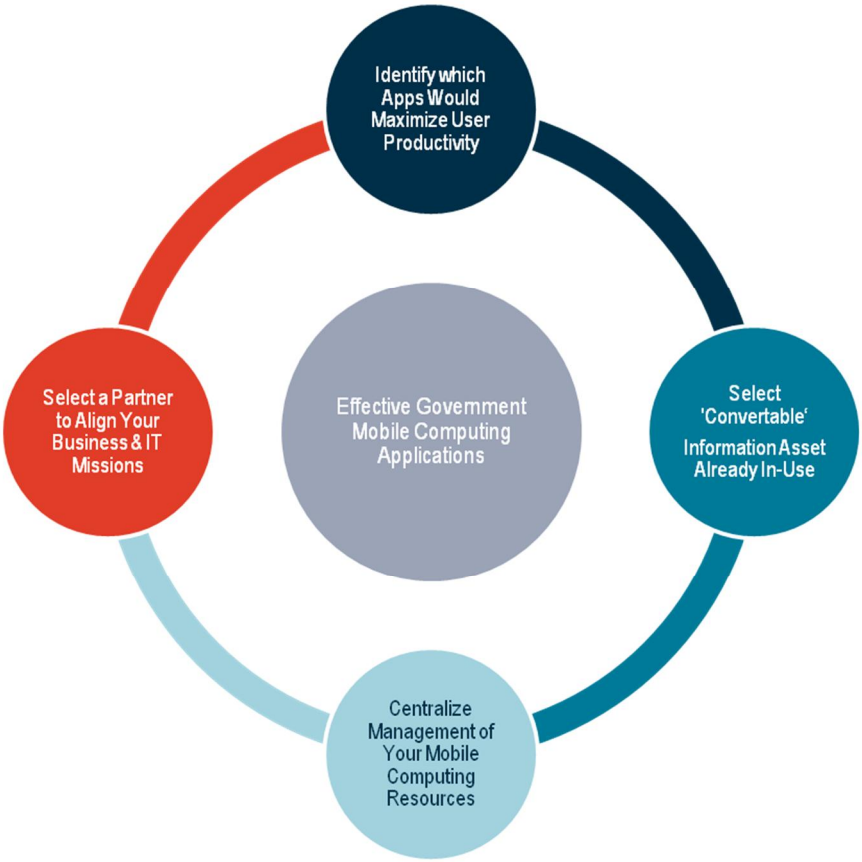

Figure 2: IntelliDyne's Strategic Impact Pillars for Deploying Effective Government Mobile Computing Applications.

[4] "U.S. CIO Unveils Mobile Strategy for Federal Government," CIO Magazine, http://www.cio.com/article/697951/U.S._CIO_Unveils_Mobile_Strategy_for_Federal_Government

STRATEGIC PILLAR 1: IDENTIFY WHICH APPS WOULD MAXIMIZE USER PRODUCTIVITY SECURELY

Your employees are mobile, and your applications should be too. Government agencies can leverage the power of mobile applications for nearly any task. Just a few of the specific uses for mobile applications include the following:

- Emergency Resource Management
- E-Commerce
- Employee Productivity
- Case Management
- Asset Management
- Field Inspection
- Biometric Identification

One of the primary uses for mobile applications for employees is telework. Many of your employees work in the field either part time or full time. Mobile applications give them access to resources, or can provide a mobile front-end to existing web-based applications. Mobile phones are already used for voice communication, but you can also expand employee communication protocols to include SMS, email, and social media applications. A survey of federal IT workers conducted by research firm Fabrizio, Ward, & Associates in December, 2011 found that 45% of respondents use mobile devices for their jobs on a daily basis.[5] It is also estimated that by the end of 2012, about 2 million federal employees will start their workdays by retrieving e-mail messages from a cloud-based system.[6] This dramatic and continuous increase in using and managing 'data on the go' presents a true challenge for any organization that plans to adapt a mobile strategy.

The greatest concern when developing a mobile strategy for employees is information security. Your employees need to work with sensitive information, and it's critical that only the right personnel can access this information. Some strategies for securing information include:

- **Understanding regulations for data security –** Every agency deals with sensitive information, and it's critical to understand the regulations and requirements for your specific agency and audience. For example, NIST has proposed specific privacy controls in response to the proliferation of mobile computing.[7] The GSA has created an initiative called Mobile Gov to "help agencies work together to make a more open, innovative government to meet 21st century citizen expectations."[8] It is important for agencies to implement solutions that are both protective and collaborative to meet privacy and ease of use as well as on-the-go efficiency requirements.

- **Requiring authentication –** By confirming identity of users before allowing a device to connect to sensitive information, you can increase the overall safety of your data. For example, there is a push

[5] Fabrizio, Ward, & Associates, December 2011
[6] "Technology: Subsidized mobile devices and other hot concepts in 2012," Federal Computer Week, January 24, 2012, http://fcw.com/Articles/2012/01/15/FEAT-Watch-List-technology.aspx?Page=2
[7] "NIST Proposes New Privacy Controls for Federal Information Systems and Organizations," NIST, July 19, 2011, http://www.nist.gov/itl/csd/privacy-071911.cfm
[8] "Mobile Government," GSA, www.gsa.gov/makingmobilegov

in the Department of Defense Health Affairs/ TRICARE Management Authority to use Common Access Cards (CAC) as an authentication method. In this case, mobile devices would need to be fitted with an external card reader.

- **Keep applications updated –** Ensure that the mobile devices used by your employees have the latest versions of applications, particularly those concerned with virus protection, encryption, or virtual private networks (VPNs). On the server side, keep your own applications updated, monitor threats, and review firewall logs to assess server security.

- **Using government-purchased mobile devices –** If you purchase your own devices, standardize setup, and distribute them to your employees, you can maintain some control over the setup and applications on the device. The downside in this case is that many of your employees already have their own personal mobile devices, and may be reluctant to carry two different phones.

- **Educating employees –** Let your employees know what they can and cannot do with their mobile devices. Inform them of the regulations relevant to your agency.

STRATEGIC PILLAR 2: SELECT 'CONVERTABLE' INFORMATION ASSETS ALREADY INUSE

While applications for your employees are important, developing applications to be used by a public audience may also be critical to your mission. Mobile applications can allow you to leverage an existing audience to provide better external communication and ease of access to information.

One approach is to tailor content that already exists in another medium, such as on a web site, to be used on a mobile device.

Two agencies that have already embraced a mobile web presence for a public audience include the Federal Emergency Management Agency (FEMA), to provide disaster updates and relief information, and the National Oceanic and Atmospheric Administration (NOAA) to provide weather forecasts and severe weather warnings. These mobile web sites are tailored for an "on the go" experience so information can be found quickly and efficiently. The Federal Government has already created a mobile apps portal to act as a central depository and access point for the public,[9] and create a specific mobile web site for finding general information about the US government.[10]

The conversion of traditional web site data into a mobile format is easy to implement for a number of reasons. First, it does not require custom code for each type of device. Any device with a web browser can access the information. Second, these applications can be integrated with device features, such as GPS for location information, for example. Finally, web-based mobile applications are easier to deploy and easier to support than stand-alone applications.

[9] "Mobile Apps," http://apps.usa.gov/
[10] "USA Gov.com Mobile," http://m.usa.gov/

STRATEGIC PILLAR 3: CENTRALIZE MANAGEMENT OF YOUR MOBILE COMPUTING RESOURCES

Whether you're developing secure applications for employees to access enterprise systems, or web-based mobile sites for public use, it's critical to centralize the management of your mobile computing resources. Enterprises need a mobile device management strategy that includes processes and tools to ensure the efficiency and accuracy of available information, device and application security, and the flexibility to accommodate user needs. It is important that mobile device management includes managing the hardware as well as the software.

The top levels of the Federal Government have already begun developing a strategy for centralizing mobile computing through the consolidation of data centers and adoption of a "cloud-first policy," as reported in a report created by then Federal CIO Vivek Kundra in December 2010.[11] The following table (Figure 3) shows that 2011 saw the Federal CIO develop a strategy for shared services within the first 12 months of execution.

	Action Item	Owners	Within 6 mos.	6-12 mos.	12-18 mos.
1	Complete detailed implementation plans to consolidate 800 data centers by 2015	OMB, Agencies	•		
2	Create a government-wide marketplace for data center availability	OMB, GSA			•
3	Shift to a "Cloud First" policy	OMB, Agencies	•		
4	Stand-up contract vehicles for secure taaS solutions	GSA	•		
5	Stand-up contract vehicles for "commodity" services	GSA		•	
6	Develop a strategy for shared services	Federal CIO		•	

Figure 3: 2011 Federal CIO strategy for shared services in first 12 months of execution.

A mobile device management strategy will provide a centralized and consistent process to control all of the mobile devices in your agency. A single process should be implemented for procurement, device setup, distribution, lifecycle management, and end of life collection. All devices should be subject to regular software updates, monitoring, and maintenance over their life cycle. All mobile users must be subject to a specific and specialized set of IT policies so you can maintain security across your network of users. These policies can be a subset of your enterprise IT policies.

Creating a central portal for self-service updates and maintenance is an effective way to streamline service and support requirements. This portal can include provisioning through enterprise application stores, remote control and support, and asset and configuration management.

[11] "25 Point Implementation Plan to Reform Federal Information Technology Management" by Vivek Kundra, US CIO, December 2010.

STRATEGIC PILLAR 4: SELECT A TRUSTED PARTNER THAT UNDERSTANDS YOUR BUSINESS MISSION, NOT JUST THE MOBILE COMPUTING TECHNOLOGY

If your agency is new to mobile computing, or if you're considering creating a cohesive mobile computing strategy for your existing applications, it may seem a daunting task to develop and implement a system-wide process that provides users with the right information and maintains security of your sensitive information. You may have the in-house resources to develop mobile applications, but do you have the expertise to implement a mobile strategy? If not, it's critical to find a trusted partner to guide you through the design, deployment, and maintenance of your mobile computing approach.

It's extremely important that you select a technology development partner that not only knows the technology inside and out, but also understands your mission. If an evaluation of a technology partner begins with questions about 'hardware and software' as opposed to questions about how to align your agency's business mission with the technology requirements, it is a tell-tale sign that the necessary and strategically difficult questions have not been asked. Knowing the right questions to ask up front will lead your agency on the right critical path to a successful mobile computing strategy.

About IntelliDyne

IntelliDyne is a consulting firm that enables better business performance through innovative technology solutions. We manage public sector programs that deliver higher operational efficiency and measurable value to clients. We advise, develop, and execute effective solutions in Cyber Security, Cloud Computing, Application Development and Mobile Computing, Business Process Management, Data Center Consolidation, Enterprise Collaboration and Enterprise Infrastructure Management.

For more information, visit our web site at www.intellidyne-llc.com or contact us at Mobile@intellidyne-llc.com.