NASCIO
Representing Chief Information Officers of the States

SECURITY AT THE EDGE: PROTECTING MOBILE COMPUTING DEVICES

PART II: POLICIES ON THE USE OF PERSONALLY OWNED SMARTPHONES IN STATE GOVERNMENT

GROWING ADOPTION, SHRINKING STATE BUDGETS, AND SAFEGUARDING SECURITY

Smartphones have dramatically grown in popularity and have commonly found their way into the government workplace. With government-issued devices, such as the BlackBerry™, iPhone™, and others, public sector employees use smartphones to access email, browse the Internet, access business applications and for a myriad of other purposes. While a great deal of productivity, efficiency and convenience can be derived from smartphone use, the potential for security incidents and data breaches is a practical concern for state CIOs and CISOs. With widespread adoption on the consumer side, state officials are now faced with a new dilemma – requests by employees to use their personal devices for state business. In an effort to address these requests, make the work lives of employees less complicated, and perhaps reduce state IT acquisition costs, officials must once again face the classic dilemma of balancing risks and rewards.

The state IT workforce is shrinking and service demands are growing. Like others in today's economic climate, state employees have extended their work day and are seeking balance between their work and personal lives. The economic downturn and shrinking state budgets have forced some states to reconsider their prohibition on the use of personal devices for official work purposes. In the past, many states managed security risks by issuing smartphones to employees and disallowing any other connection to networked resources so that the state had control over how smartphones were configured and used. But not every state can afford that kind of control and many have cut costs by limiting the number of employees who receive work phones. As a result, many employees have tried to stay connected by

NASCIO Staff Contact:
Charles Robb
NASCIO Senior Policy Analyst
nascio@amrms.com

Chad Grant
NASCIO Policy Analyst
nascio@amrms.com

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

transforming their personal smartphones into a combination of business and non-business use.

As part of their broader security framework, CIOs and CISOs must establish expectations for use of state and non-state owned mobile tools.[1] The guidelines should indicate if certain devices are permissible and if so, what information, data, and records can be maintained outside of a secure environment. In response to inquiries from Delaware and Nebraska, NASCIO conducted a survey to provide an overview of how states have addressed the use of personal smartphones and to highlight policies that ensure security is a key component in considering mobile and wireless technology and services.

ANTICIPATING WIDESPREAD USE

In July of 2009, NASCIO addressed the growing presence of powerful mobile computing devices in the workplace. The brief, *Security at the Edge — Protecting Mobile Computing Devices,* highlighted the risks that accompany such devices as they make their way into the workplace. According to a NPD Group report, smartphone penetration reached 31% of the U.S. population in 2009, compared with 23% a year earlier.[2] Whether they enter the system through either authorized or informal paths, the brief emphasized that states information security programs must manage the increased risk associated with those devices.

The state CIO must anticipate efforts to reduce costs in government spending and the challenges that come with it, both in terms of line-of-business desires to reduce operational costs and the simple abundance of personal smart computing devices.

The question still remains, however: are security measures for personal smartphones, coupled with use policies, rigorous enough to allow these devices to be used for government business?

APPROACH AND HIGHLIGHTS

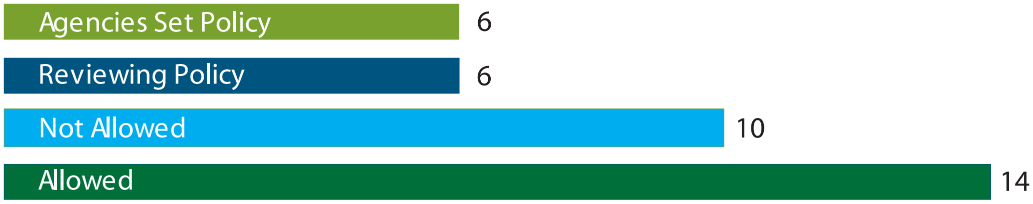
This update to *Security at the Edge*, with a focus on use of personal devices in state government, was designed to survey state policies and security measures for use of personal smartphones connecting to government networks. In an effort to gain a general overview of the use of personal smartphones for government business purposes, NASCIO conducted a survey of its members: the states, territories and the District of Columbia. While state policies, standards and security provisions are evolving for the use of personal smartphones, there is significant interest in the topic–36 states responded to NASCIO's query.

Definition of "Smartphone"

While there is no industry standard that defines a smartphone, they typically handle multiple e-mail accounts (including government types), have a sophisticated organizer, and can handle electronic documents. Some allow creation and editing of spreadsheets and documents, and they usually come with personal information management software for use with PCs. Their advanced operating systems give them access to a host of applications: productivity tools, shopping, multimedia, games, travel, news, weather, social, finance, references, etc.[3] Many of the smartphones also have cameras, audio capabilities, and a location tracking function that complements and consolidates several devices into one.

Gartner defines a smartphone as "A large-screen, voice-centric handheld device designed to offer complete phone functions while simultaneously functioning as a personal digital assistant (PDA)."[4] In addition, Computer World's January 18, 2010 cover story "Smart Phones Need Smart Security" concluded that "smartphones should be viewed not as phones but as PCs that happen to make phone calls."[5] The varying definitions highlight the fact that smartphones are increasingly powerful devices that are continuing to evolve around consumer-centric needs.

FIGURE 1: STATE OF THE STATES FOR PERSONAL SMARTPHONE USE (36 STATES)



- **39% (14 states)**, stated that they allow the use of personal smartphones for government use and have implemented security measures to protect the state from breaches. Delaware is one of the states that have witnessed a shift in requirements from their employees, trending toward synchronizing their work email and calendars to their personally owned smartphones. To date, they have approximately 150 users doing this by using a standard browser to navigate to Microsoft Outlook Web Access and also using a free service (ActiveSync) to transport documents, calendars, contact lists and email to the smartphone.

- **27% (10 states)**, reported that they currently do not allow the use of personal smartphone devices for state government use. The reason that many of the states do not allow this is because of requirements to use pre-approved government issued devices.

- **17% (6 states)**, reported that each state agency has its own policies and guidelines. An issue to consider is that as many states begin IT and email consolidation efforts, this may be a topic that needs to be revisited as part of establishing an enterprise policy.

- **17% (6 states)**, conveyed a great interest on the topic of personal smartphones and are currently in the process of reviewing state policy.

BREACHES IN SECURITY

The September 2008 brief, *Protecting the Realm*, noted that many data breaches have resulted from lost or stolen mobile devices, and that the encryption of information both at rest and in transit has become one way that states and other entities have addressed data protection concerns with mobile devices.

The lost-device issue list from *Protecting the Realm* noted that:

- The nature of the information/data may be highly sensitive.
- The nature of the information/data on the device may be unknown.
- The information/data may not be backed up, or if backed-up, may not be backed up on enterprise servers.
- The information/data may include non-business related material which is inappropriate for maintenance on a state-owned asset.
- The information/data may have resided on a personal device owned by the end-user, rather an on a state-owned asset.
- Encryption may not be employed or, if employed, may not meet enterprise standards.
- Password protection or other authorization/access control mechanisms may not be in place, or again may not meet enterprise standards.
- The device may not be subject to remote wiping.
- The device may or may not be on an asset inventory, or the inventory may not be integrated with that of other IT assets.

- Users may be unaware of appropriate use and security requirements associated with mobile devices.
- Use of the device over WiFi networks may be insecure.

As mobile device technology continues to advance, it is probable that smartphones could become the primary computing platform for an individual.[6] In anticipation of a more abundant use of smartphones, several states have established enterprise policies for security standards and conditions of use for personally owned devices. Although challenging because of vulnerability to theft or being misplaced, and the commingling of business and personal information, applying security controls on personally owned smartphones is a feasible solution to protecting the security of government networks.

BALANCING THE RISK AND PREPARING FOR THE WORST

If a state is going to permit non-government-issued smartphones to be used in the workplace, there are steps that need to be taken to provide adequate security measures.

- **Extend enterprise security policies to encompass personal devices used for business purposes.** To the extent possible, State CIOs must formally extend security policies, standards, and guidelines to address use of personal devices and supersede inconsistent agency level policy standards that may cause a threat to the integrity of the government network.

- **Acquire security software.** Requiring employees who use their smartphones to access the network to use security software on that phone. Security suites provide features such as encryption, antivirus, firewalls, and other essential protections. Some can even be set up so that phones are required to have a firewall active before they can connect to the network.

- **Use password protection.** Most smartphones and their operating systems have the ability to set up the phone to be password-protected. This is something that should be explicitly required.

- **Enable remote wiping.** If a user loses his or her phone, remote wiping allows the data on that phone to be erased from the office. The employee, of course, must be made aware of this requirement prior to being authorized to use the device for business purposes.

- **Disable unnecessary features.** For example, require users with Bluetooth to disable the broadcast mode so that others can't discover and attack that phone via Bluetooth.

- **Give smartphones only appropriate access.** Set policies so that certain databases, applications, or documents cannot be accessed by phone. That way, even if an employee loses his or her phone, only a limited part of the network will potentially be vulnerable.[7]

* Delaware: Balancing Business Needs Without Compromising Security

In response to a shift in requirements from state employees, trending toward synchronizing their work email and calendars to their personally owned smart phone, Delaware has laid out a framework for enterprise security. With a proposed cutover date of mid-July 2010, the state plans to implement its own policy on personally owned smartphones and has not disabled this capability in the interim.

There are two ways synchronization is being achieved in Delaware:

1) using a standard browser to navigate to Outlook Web Access (OWA)
2) using a free service (ActiveSync) to transport documents, calendars, contact lists and email to the smartphone

The OWA option uses standard browser "pull" technology and the permanent home of the data is on server(s) that the state maintains and secures. In contrast, the ActiveSync option uses "push" technology to send data from the server to the smart phone. In the event that the phone or removable memory card is lost, stolen, sold, or even taken in for repairs, having minimum security controls in place will help protect the state network and data from breaches.

The following measures have allowed Delaware to balance business needs without compromising security:

- Continue the use of the Blackberry as the state supported and approved business mobile device.
- Continue offering the standard browser-based OWA service.

- **Enforce security policies.** Once mobile device policies have been established, it is important to check for compliance. The states must have faith in the devices connected to the network are secure, but also verify security precautions meet expectations.

RECOMMENDATIONS FOR PERSONAL SMARTPHONE USE

- Recognize the increased prevalence of personal smartphones in the marketplace and the ever expanding capabilities of these devices. As storage and access capacities increase, guidelines should be established to assert what type of information can be securely protected.

- Reduce costs and manage expectations by establishing an enterprise policy on the use of personally owned smartphones. The convenience of a single device for state workers is very enticing, but clear security controls and end-user responsibilities must be agreed to.

- Embrace the business capabilities of smartphones, but only allow devices that can be provisioned to meet appropriate security standards. In addition, states will need to contemplate what is acceptable use for smartphones and if an employee has expectations for reimbursement.

- Set expectations for the end-user because inevitably smartphones may be lost or stolen. Reporting the loss of a device or a data breach to an IT agency will increase the chances of securing information and data.

- Mitigate risks by using the proper tools to improve mobile device security. Smartphones should be required to have encryption capabilities to protect stored data, strong passwords, inactivity timeouts, lock out after several failed attempts to log in and remote whipping capabilities.

- Anticipate there will be problems that will arise and troubleshoot connectivity and security issues on personally owned smartphones.

As states continue to balance cost controls and advocate for the enterprise focus on IT, there are clearly innovative technologies, strategies and tactics for reducing and avoiding costs. The use of personal smartphones in the workplace may be a viable option to consider. NASCIO urges CIOs and CISOs to examine the states that allow personal smartphones and to build upon their experiences to establish enterprise policies and practices that protect the network, applications, data and devices from security breaches.

- Continue offering the ActiveSync service but only for mobile devices that can be provisioned to support the policy.
- Amend the Portable Wireless Network Access Device Policy to require that mobile devices that connect to the exchange must accept Delaware's security configuration.
- Customers will register their devices with Delaware and digitally sign off acknowledging that they agree to the following minimum security controls. These controls mirror Delaware's Blackberry policy and can not be disabled by the user:
  - Strong passwords/history
  - Password expiration
  - Lockout after several failed attempts
  - Encryption
  - Inactivity timeout
  - Remote wiping for lost/stolen devices
- Mobile devices that can not be provisioned to support the policy will not be allowed to connect to the state's email system.

In addition, Wisconsin is taking a very similar approach on the use of personally owned devices and Indiana and Minnesota appear to also be leaning toward implementing comparable policies and standards.

APPENDIX A - WHICH STATES ALLOW THE USE OF PERSONALLY OWNED SMARTPHONES FOR GOVERNMENT BUSINESS? (33 STATES)

STATE	RESPONSE	POLICY COMMENTS	DEVICE
Alabama	Allowed	When communicating with state systems personally-owned PDA's shall comply with the requirements stated in Alabama Information Technology Standard and other applicable state standards	n/a
Alaska	Allowed	All employee owned assets used for state business must comply with state security standards	n/a
Arkansas	Agencies Set Security Policy and Guidelines	Legislation was passed requiring agency directors to create policies prohibiting the use of personal equipment without prior approval	n/a
California	Reviewing Policy	State agencies seem to have differing interpretations on the intent of the policy and California would like to review its policies	n/a
Colorado	Reviewing Policy	Colorado's is in the process of reviewing its policy	n/a
Delaware	Allowed	Delaware has seen a shift in requirements from their customers, trending toward synchronizing their work email and calendars to their personally owned smartphone. To date, they have not disabled this capability and have approximately 150 users doing this today. There are two ways this synchronization is being achieved: 1) using a standard browser to navigate to Outlook Web Access (OWA) 2) using a free service (ActiveSync) to transport documents, calendars, contact lists and email to the smartphone	Not indicated
Florida	Allowed	Florida allows the use of personally owned devices	n/a
Hawaii	Allowed	Hawaii allows personal Blackberry devices to participate, but they must accept a pushed security policy. Hawaii does allow personal devices to access e-Mail via the web	Blackberry
Idaho	Reviewing Policy	Idaho is still determining how they set policy standards for personally owned devices	n/a
Indiana	Allowed	Indiana allows personal smartphones as the enterprise moves to Exchange 2007, seems it provides necessary controls	Not indicated

Iowa	Agencies Set Security Policy and Guidelines	Each agency has its own policies and guidelines. As Iowa begins the IT and e-mail consolidation process, they anticipate revisiting this topic and creating an enterprise policy	n/a
Kentucky	Agencies Set Security Policy and Guidelines	Kentucky sets policy at the agency level	n/a
Maine	Not Allowed	Only Blackberries are allowed and personal Blackberries would require a CIO waiver. Block all other personal devices	Blackberry
Maryland	Allowed	Maryland allows the use of personally owned devices but prior written approval by the CIO or other delegated authority of the executive departments or independent state agency. If approved, the user may be granted restricted network access rights and is required to provide protections equivalent to the agency's protection of its own equipment	n/a
Massachusetts	Not Allowed	All wireless mobile communications devices that connect to the Commonwealth LAN/MAGNet must be the property of the Commonwealth. No personally owned wireless mobile communications devices or vendor equipment may connect without express written permission of the Executive Department CIO	n/a
Michigan	Allowed	Michigan allows the use of personally owned devices	n/a
Minnesota	Reviewing Policy	Minnesota is currently reviewing its personally owned devices policy and anticipates moving toward allowing use with certain security measure in place	n/a
Mississippi	Allowed	Mississippi allows access on a limited basis, but are actively investigating broader use	Not indicated
Missouri	Allowed	Missouri has just started letting employees use personally owned devices, but require the same security standards as a government issued device	Not indicated
Montana	Allowed	Mobile devices have to comply with Exchange Security Configuration (ESC) policy, and must be connectible through Windows Active Sync software. The state of Montana does allow personally-owned devices	n/a
Nebraska	Not Allowed	Standing law that excludes the personal use of state resources and networks	n/a
Nevada	Allowed	Agency manager works with the employee to establish appropriate physical and data security controls for mobile devices that are approved to contain state data	n/a

New Jersey	Agencies Set Security Policy and Guidelines	New Jersey’s agencies currently set policies regarding devices, but the there is an interest in reviewing the personally owned devices provisions	n/a
New Mexico	Reviewing Policy	New Mexico is currently reviewing it policy on personally owned devices	n/a
New York	Agencies Set Security Policy and Guidelines	New York agencies have discretion to establish their own set of policies	n/a
North Carolina	Allowed	North Carolina allows personally owned devices to be used for business purposes. North Carolina is also working to expand its guidance on the use of personally owned smartphones	n/a
Oregon	Not Allowed	Under the Enterprise Acceptable Use policy each agency is able to make their own decision on use of smartphones	n/a
Rhode Island	Not Allowed	In Rhode Island no personal devices are allowed on government network	Not indicated
South Dakota	Not Allowed	State-only devices	Blackberry
Tennessee	Not Allowed	No personal devices attached to state resources, only sync available is with state-supplied Blackberry's	Blackberry
Utah	Agencies Set Security Policy and Guidelines	In the process of investigating this topic further	n/a
Virginia	Agencies Set Security Policy and Guidelines	Each agency or their service provider must determine and document whether personal IT hardware assets should be allowed onto premises that house COV IT systems and data based on agency’s unique operating environment and needs. Personal IT hardware assets should be prohibited unless there is an identified unique business need, which should be documented to include the need, risks, controls and unmitigated risks	n/a
Washington	Not Allowed	Each agency is tasked with adherence to state policies and Washington does not allow personally owned devices to be connected to the state network	n/a
West Virginia	Not Allowed	Forbids use of personal smartphones	n/a
Wisconsin	Allowed	Moving from Blackberry devices to Windows mobile devices. Wisconsin allows the use of personal phones, due to demand and costs. Device must be wipe-able	Windows mobile
Wyoming	Not Allowed	Blackberry, state-owned only, no personal devices	Blackberry

APPENDIX B - ENDNOTES

[1] See < http://www.nascio.org/publications/researchBriefs.cfm >, July 2009.

[2] See < http://www.npd.com/press/releases/press_100317.html >, March 17, 2010.

[3] See < http://www.consumerreports.org/cro/electronics-computers/phones-mobile-devices/cell-phones-services/cell-phone-service-buying-advice/cell-phone-service-types/cell-phone-service-types.htm >.

[4] See < http://www.gartner.com/6_help/glossary/GlossaryS.jsp >.

[5] See < http://www.computerworld.com/s/article/345297/Smartphones_Need_Smart_Security >, January 2010.

[6] See < http://www.digitaltrends.com/features/the-future-of-smartphones-2010-2015-and-beyond/ >, February 2010.

[7] See < http://www.processor.com/editorial/article.asp?article=articles%2Fp3120%2F27p20%2F27p20.asp >, July, 2009.