NASCIO Representing Chief Information Officers of the States

Research Brief

September 2005

NASCIO Staff Contact: Mary Gay Whitmer, Issues Coordinator, mwhitmer@amrms.com or (859) 514-9209.

The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Part II

Overview

The conclusion of Part I of this Research Brief presented five scenarios with potentially negative consequences for citizen privacy that, if not addressed, could outweigh the mobility and productivity benefits that wireless technologies bring to the state government workplace. Part II of this Research Brief offers guidance to states for developing and implementing privacy policy measures and securing wireless technologies, such as wireless local area networks (WLANs) and personal digital assistants (PDAs). Part II's goal is to prevent the unauthorized exposure of citizens' personal information. It also addresses ways that states can implement emerging wireless technologies, such as geo-location and Radio Frequency Identification (RFID) tagging, in a manner that is not invasive to citizens' perceived privacy expectations.

Why This is Important for State CIOs:

The Benefits of Wireless Technologies: From wireless PDAs to laptops to smart phones, many wireless technologies are allowing state employees to stay productive while on the go. States are also providing more services to citizens through wireless technology applications such as subscription-based email notifications. However, if citizen or state employees' personal information is transmitted by or stored on wireless technologies, such as PDAs, the possibility for the compromise of that information is created. The proper privacy and security measures, though, can prevent the unauthorized exposure of citizens' personal information.

The Importance of Protecting Privacy: *The goal of this Research Brief is to help states implement wireless technologies that provide improved mobility, business processes, and citizen services without creating circumstances that are ripe for the exploitation of the personal information that is used and stored in many state agencies.* Avoiding instances in which that information is exposed to unauthorized parties or identity thieves will foster citizen trust in states' ability to collect and use citizen information without compromising privacy. Although this brief refers to "citizens' personal information," implicit within that umbrella term is the personal information of state employees. States have a duty to protect the personal information of their employees in the same way that they have a duty to protect the personal information of citizens. The protective measures suggested in this brief can also be used to ensure the privacy of state employees' personal information.

The Role of the State CIO: The recent string of data breaches, both in the public and private sectors, demonstrates the high-profile consequences that may occur when an entity fails

to live up to citizen expectations of privacy. This is particularly important because mobile wireless devices may store and/or transmit sensitive information. For example, a recent Symantec study indicated that 37% of users of smart phones for business purposes store confidential information on those devices but only 40% of the companies surveyed have wireless security policies. *State CIOs have an important role in ensuring that wireless technologies provide the intended mobility, business process and citizen service benefits without resulting in compromised citizen privacy and harm to citizens' trust in the state's ability to keep their personal information safe.*

Recommendations for Unauthorized Exposure Risks

General Measures:

- **Recognize the Enterprise Risks:** States must understand that a single agency's implementation of a wireless technology can compromise the entire state network if not properly secured. Such security breaches could place at risk sensitive or confidential information transmitted over the state network. *The State CIO can play a valuable role in ensuring that security and privacy policies are in place and that all agencies comply with those policies.*
- **Start Risk Assessments Early!** Regardless of the origin of the privacy risk, states should assess, identify and address wireless technology privacy risks in the planning and design stages. Steps early in the process will help to avoid high-profile privacy problems later on. States can build this analysis into their information assurance programs, which ensure the confidentiality, integrity, availability and authenticity of state information and IT systems.
- **Data Classification:** *Data classification programs can greatly assist states in determining which categories of information require greater levels of protection from unauthorized exposure.* Information that does not include citizens' personal information may not require the same types of security measures, such as encryption, that personal information requires when transmitted by or stored on wireless technologies. As part of its overall IT security strategy, Washington State requires agencies to classify data, whether transmitted wirelessly or otherwise, into at least two categories—confidential and public. Confidential information is afforded higher levels of protection to ensure its privacy.
- **Develop Wireless Technology Policy Provisions:** States should develop privacy and security policy provisions that apply specifically to wireless technologies. These provisions may be included in a state's overall IT security policy. They should address the processes agencies use to evaluate wireless technology risks and the mitigation of those risks through privacy, security, and other precautionary measures. Such policy provisions should also identify acceptable uses of wireless technologies in the state government workplace. Compliance should be mandatory.
- **Ensure that Your Wireless Policy Provisions are Inclusive:** A state's wireless technology policy should be broad enough to encompass the variety of technologies that are currently available in the market and those that might be on the horizon. Michigan has identified seven major types of wireless technologies:
    - Point-to-Point (Building-to-Building)
    - Local Area Network (LAN) Access Points
    - Cellular
    - Wireless Email (e.g. Blackberry)

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

  - Personal Area Networks (PAN) including Bluetooth
  - Remote public wireless hot spot access points
  - Wireless LAN cards.
- **Training:** *Employees and IT contractors should receive training pursuant to the state's wireless policy provisions so they understand how and when they may use those technologies*. Training is especially important for difficult-to-secure devices, such as Bluetooth-enabled devices, that may participate in ad hoc networks or have continuous network connections.
- **Prohibiting Certain Types of Information from Entering the Wireless World:** For some types of highly sensitive information, the ramifications of a privacy breach may be so severe as to warrant prohibiting that information from being transmitted by or stored on wireless technologies in the first place. For example, the federal government restricts tax information from being transmitted via wireless technologies. Some states also restrict the wireless transmission of highly confidential or sensitive health information.
- **Carefully Weigh the Risks and Benefits:** Since wireless technology privacy and security measures are still maturing, states should carefully assess the risks and benefits of implementing wireless technologies. This is especially important for mission critical systems for which wireless technology would not add substantial benefit. States may choose to hold off on implementing wireless technologies for such systems until wireless security has matured.
- **Limit the Use of Wireless Technologies to Those Who Need It:** Allow only those who need a wireless device to have it. Michigan limits the use of wireless technology to instances in which it meets the unique needs of an agency's business requirements and where the expenditure of resources necessary to secure the device or technology is justified.
- **Concerns with State IT Contractors:** In recent years, there has been an increased pressure to "in-source" core IT functions that may have been performed by contractors at one time. *With outsourcing forecast to grow again because of service demands, states should take the same steps to train contractors as they take to train state employees on the acceptable use of wireless technologies.*
- **Do You Know Where Your Wireless Devices Are?** States should require that agencies inventory and document all wireless assets and devices. If a state implements new wireless policy provisions, the state should also require agencies to inventory and document all wireless assets and devices. In this way, the State CIO can ensure that agencies are compliant with the new wireless policy requirements. Thereafter, agencies should periodically inventory their wireless assets.
- **General Security Measures:** As with wired technologies, states should employ adequate security measures, such as anti-virus, anti-spyware, and firewall protection. Moreover, states should consider encryption and authentication where the privacy risks to sensitive information warrant.
- **Don't Forget Physical Security Measures:** Agencies should be required to develop policies to physically secure wireless devices from compromise. For example, a stolen laptop with personal information could place citizens at risk for identity theft. Washington State requires agencies to address these issues in their internal IT security policies. North Carolina's wireless policy provides for wireless access points and related equipment to be secured with a locking mechanism or kept where access is restricted to authorized personnel. The ability

to remotely deactivate portable wireless devices can also help protect sensitive information on those devices if they are stolen or misplaced.

- **Gauge Security Measures to Address a Wireless Technology's Risk Level:** Some uses of wireless technologies may present greater risks than others. States should carefully evaluate the risks and then implement the appropriate security measures to address those risks without resulting in security "overkill." To avoid this, Michigan characterizes wireless technologies according to security zones. Different zones require different security measures. For the "trusted zone," any access beyond Internet-available web applications requires the use of a Virtual Private Network (VPN) and two-factor authentication. The trusted zone also requires heightened security measures for LANs and wide area networks (WANs), including "centrally managed access to the network."
- **The End of the Life Cycle:** Wireless portable devices should be included in the state's surplus equipment and disposal lifecycle requirement. The state should ensure that all data is permanently removed from those devices before they are returned to the vendor or otherwise surplused.
- **Involve Procurement Officials:** Those within a state's procurement office who are responsible for purchasing wireless technologies must be familiar with the state's wireless IT policies. This will help them to ensure that the purchased wireless technologies meet the required specifications.
- **Enforce Agency Compliance:** It only takes one state agency to falter on compliance with a state's wireless requirements to compromise sensitive information either on the wireless or wired network. Hence, periodic assessments and audits are necessary to monitor compliance and identify and remedy any instances of noncompliance.
- **Educate and Enlist the Help of IT Vendors:** States should raise awareness among wireless technology providers within the vendor community. Wireless providers should understand the protective measures that their technologies must possess in order to meet the state's privacy and security expectations. With that level of understanding, vendors will also be able to help educate those within the state as well as other vendors.

Beware of the War-Drivers--Unauthorized Exposure Risks:

Overview of the Risk: If not properly protected, wireless networks and devices can place transmitted information at risk for access by unauthorized parties. For example, one potential threat is hackers called "war drivers" who park outside office buildings and intercept wireless signals. If personal information is intercepted, it could place citizens at risk for identity theft. Public wireless "hot spots" can also pose risks in terms of exposing personal information, since hot spots normally can be used by anyone.

Wireless Privacy Risk Scenario #1: Will war drivers parked outside a state office building be able to intercept sensitive information transmitted over the state's wireless network?

A Solution: States should be aware of how far access point signals extend and whether they exceed the building's perimeter. Access points should be configured in a way to avoid signal leakage outside of the building's perimeter if technically feasible. States can also protect sensitive information with encryption technology, so that, if intercepted, the intercepting party will not have access to the content of the wireless transmission.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Recommendations:

- **Reporting of State Agency Wireless Local Area Networks (WLANs):** *The State CIO should be aware of all agency WLANs to ensure that they are compliant with the state's wireless policy provisions.* North Carolina, Kentucky and other states require that all WLANs be reported to the State CIO.
- **More on Data Classification:** Prohibiting highly sensitive classes of information from transmission by or storage on wireless technologies can help states avoid privacy breaches with serious consequences, such as the release of highly sensitive medical or government security information. This is consistent with the approach of the National Institute of Standards and Technology (NIST). That organization recommends that agency policies address the specific types of information that may be transmitted over wireless networks.[1] Agencies should then develop access security controls that are consistent with their data classification policy.
- **Encryption:** Encryption protects the content of sensitive information if intercepted by unauthorized individuals. Whether encryption is needed depends upon the sensitivity of the information involved. NIST anticipates that wireless encryption will improve in the coming years, which will help counter the risks presently posed by eavesdroppers on wireless networks.[2] Washington State, for example, requires encryption for transferred or emailed confidential data. Encryption at multiple layers may also be necessary. For building-to-building implementations, Michigan requires connection point node-to-node router level encryption from the nearest connection routers in addition to wireless media encryption.
- **Authentication:** Many types of wireless devices from laptops to PDAs may be used to connect to a wireless state network. Device and/or user authentication can address the problem of unauthorized individuals connecting to a wireless state network to snoop on the sensitive information. In Michigan, security measures for wireless networks include two-factor authentication methods. Moreover, authentication not only can be used for wireless devices but for access points as well. North Carolina requires authentication when point-to-point access is used between routers to replace traditional common carrier lines.
- **The Virtual Private Network (VPN) Option**: The use of a VPN may be helpful if employees typically use their laptops and a public wireless hot spot to connect to the state network. A VPN uses tunneling protocols to encrypt data sent through a wireless connection. Only properly encrypted data can enter the VPN tunnel. However, to ensure data protection even with the use of a VPN, Michigan requires personal firewalls for all VPN connections.
- **Other Security Measures**: Firewalls, anti-virus and anti-spyware protection, audit trails, hardened passwords, disabling Simple Network Management Protocol (SNMP), and other security measures can help protect the wireless network from unauthorized individuals who threaten the privacy of sensitive information transmitted over the network.

[1] "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," Special Publication 800-48, Tom Karygiannis and Les Owens, NIST (National Institute of Standards and Technology), (November 2002), <http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.>.
[2] Ibid.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Recommendations for Access Points: Wireless LANs, computers and other devices enabled with wireless network adaptors are connected to the wireless network via an access point. The typical coverage area of an access point is up to 300 feet, which allows employees to use their wireless devices from any location within the coverage area. Access point coverage areas can be linked together so that employees or guests may use their devices anywhere in a building or from building-to-building. Recommendations for securing access points include:

- **Monitoring for Rogue Access Points:** States should frequently monitor for the installation of rogue or unauthorized access points on the wireless network. A WLAN's management software may provide for rogue access point monitoring, and sniffer technologies may be used as well. Management systems should also monitor the airspace for rogue access points.
- **The Right Configurations are Not Always the Default Configurations:** Access points have default configurations that are enabled by the manufacturer. States should not assume that access points are properly configured out-of-the-box. Prior to installation, access point configurations should be examined and changed if necessary to ensure that protective measures are active and maximized.
- **SSIDs:** The Service Set Identifier (SSID) is a value that identifies an access point. Access points usually come from the manufacturer with a default SSID. However, many default SSIDs are well-known and make it easy for wireless devices to guess the SSID, thereby gaining access to the network. North Carolina requires that an SSID be changed from the default value and must not contain characters indicating access point location or agency or other identifying name. Where technology permits, the SSID's broadcast function should be disabled so that devices wanting access to the wireless network must provide the correct SSID before connecting.
- **Other Security Precautions:** North Carolina requires that the access point reset function can only be used and accessed by authorized personnel and that administrative personnel provide the correct password in order to gain access to administrative features.

Beware of Prying Eyes--Exposure in Storage:

Overview of the Risk: States' vast amounts of citizens' personal information stored on wireless devices must be protected from identity thieves and unauthorized employee snooping. This is especially a concern with the increased prevalence of smart phones, wireless PDAs, laptops and memory sticks. Since these devices are small and compact, they are especially susceptible to accidental loss or theft. State employees also may purchase these devices on their own and use them for both personal and business matters.

Many of the measures used to protect stored sensitive information on wireless devices are the same as those used to protect against other wireless risks, such as the unauthorized interception of wireless transmissions. Some of these measures include:

- Developing enterprise policy requirements that cover wireless portable devices
- Conducting data classification activities and identifying the types of information that may be stored on wireless devices
- Changing default configurations on wireless devices to maximize security and privacy protections

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

- Installing and managing firewall, anti-virus and anti-spyware protections on devices capable of handling those protections
- Enabling audit features to track device connections and Internet activities, and
- Inventorying and keeping track of all state-issued wireless portable devices.

Wireless Privacy Risk Scenario #2: Will the state be able to stop an employee from connecting to a public wireless hot spot in an airport coffeehouse via an improperly configured state-issued PDA, thereby allowing a nearby hacker using the same hot spot to compromise sensitive information on the state employee's PDA?

A Solution: In this instance, the most fool-proof solution is to monitor and prohibit the storage of sensitive information on PDAs and similar devices. States may also choose to limit the use of wireless devices with sensitive information outside of the state workplace except where absolutely necessary. However, if that approach is not feasible, then the state must make sure that wireless portable devices are properly configured before placement in the hands of employees. A state's wireless requirements can provide guidance on proper configurations. Sensitive information should also be encrypted, and employees should be required to complete security awareness training prior to using such devices.

An alternative solution may be for the state to limit the autonomy of wireless devices by using them primarily as thin clients that do not store information. In that case, employees would connect to the state network via those devices and place and use any sensitive information on the network without storing it on the wireless device itself.

Recommendations:

- **Match the Wireless Technology to the Employee's Work Needs:** Given the prevalence of wireless devices for both professional and personal use, states should carefully determine which employees have a legitimate business need for wireless devices. Only those with a legitimate business need should be issued state-owned wireless devices. Potential privacy exposures can be further minimized by matching the capability of the wireless device to the employee's work requirements. For example, employees in managerial positions are typically message-oriented and may only need remote email and calendar access. Others, such as field inspectors, may need more robust network coverage and mobile access to online databases to complete forms in the field.
- **Personal Devices Used for Business Purposes:** Since some employees may use their personal wireless devices for business purposes, states should consider requiring employees to comply with wireless policy requirements when using their personal devices to conduct state business. For instance, Washington State requires agencies to develop, document and implement policies and procedures that require any remotely attached device, either employee-owned or agency-owned, to have current patches. If an employee is not in compliance, access to the state network may be blocked.
- **Addressing the Length of Storage of Sensitive Information:** A state's wireless policy requirements should address how long sensitive or personal information may be stored on a wireless device. As a general principle, sensitive information should be stored for only as long as it is needed. For wireless PDAs and similar devices, information can be archived on

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

a fixed, wired device, such as a desktop computer or file server, and placed back on the wireless device if needed later on.

- **Monitor for the Installation of Unauthorized Applications or Programs:** An employee's installation of a program or application on a wireless device could inadvertently lead to the installation of spyware or other types of malicious software that monitor and extract personal information. To avoid this, state employees should be required to request clearance from the appropriate IT personnel before installing any new programs or applications.
- **Education is Never a Waste!** Even if a state employee is aware of privacy and security precautions with respect to desktop computers, the employee may not realize that those and other risks extend to portable wireless devices. States should educate employees regarding the acceptable use of wireless portable devices for transmitting and storing sensitive information. For example, employees should be made aware that the synchronization of a wireless PDA with a desktop computer can create vulnerabilities that could lead to the exposure of sensitive information stored on the PDA.
- **Ad Hoc Network-Enabled Devices:** Additional training may be needed for devices that can connect to ad hoc networks, such as those that are Bluetooth-enabled. Those devices may have interface and Internet connection capabilities that could allow unauthorized parties to access information on the device even when the device is not in use. Michigan requires that Bluetooth-enabled devices only be used in secure areas with the highest security settings and provides additional security awareness training for individuals with those devices.

Recommendations for Portable Wireless Devices:

- **Encryption:** After determining whether any sensitive information may be transmitted by or stored on portable wireless devices, states should examine whether and what type of encryption is needed to protect various categories of sensitive information when stored or transmitted by wireless devices. If stored information is sensitive and requires encryption, states should be sure to purchase devices that are capable of encrypting stored information. North Carolina prescribes the type of encryption that is appropriate for different types of information. For non-confidential information, encryption in accordance with the Wi-Fi Protected Access (WPA) standard is acceptable, while WPA2, the latest version of the WPA standard, should be used for confidential information. That state's policy also provides that the Wired Equivalent Privacy (WEP) standard, which was the original Wi-Fi security standard, should not be relied upon for wireless security.
- **Passwords and PINs:** Passwords or PINs used to access a portable wireless device should be required as another layer of protection for information on lost or stolen devices.
- **Locking Mechanisms:** States should purchase wireless portable devices that have the capability to automatically lock if not used for short periods of time and shut down when not used for extended periods of time (except where continuous network connectivity is intended). Michigan's security standard embodies these precautions.
- **Immediate Employee Reporting of Lost or Stolen Devices:** Must be a state requirement.
- **Remote Deactivation:** States should require features that allow IT administrators to remotely deactivate wireless portable devices. This can prevent sensitive information on those devices from falling into the wrong hands.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Shut the Back Door--Exposure of the Wired Network:

Overview of the Risk: Employees' use of wireless devices, such as PDAs, also can be a vehicle for compromising personal information transmitted by a state's wired network. As wireless portable devices have become smaller, yet more powerful, they now present a risk to the state's wired network. Such devices can easily and surreptitiously steal information transmitted by the wired network or stored on office desktop computers or servers.

Wireless Privacy Risk Scenario #3: The state's human resources agency has terminated an employee but failed to deactivate his state-issued wireless PDA prior to the termination. Will the terminated employee retaliate against the state by plugging his still activated PDA into an office computer and taking with him the personal information of state employees, including SSNs and health insurance and background check information?

A Solution: The first step in preventing this scenario is to ensure that all state-issued wireless devices can be remotely deactivated. The state should also have a policy that provides for deactivation immediately before actual notice of termination to the employee.

* * * * *

Wireless Privacy Risk Scenario #4: A state employee who loves the latest technology gadgets receives a nifty new wireless PDA (with a substantial memory capability) from his wife for his birthday. He immediately starts using it for not only personal matters but also for state business purposes, including the storage of files containing citizens' Social Security Numbers. He does not inform his state employer about his new PDA.

A Solution: A state's wireless policy provisions should address employees' use of their personal devices for business purposes. The state should provide any circumstances under which such uses are acceptable and address if and when sensitive information may be stored on those devices. However, this could present substantial problems, because a state may not be able to remotely deactivate or erase the memory of such devices if they are not state-owned. At a minimum, employees should be required to have and regularly update their personal wireless devices' security measures, such as anti-virus, anti-spyware, and firewall protection.

Recommendations:

- **Evaluate the Design of the Wired Network:** States should carefully examine the design of their wired networks in order to identify vulnerabilities that could be exploited by wireless devices. One design option is to allow limited entry points to the wired network by wireless devices. *This may include requiring agencies to seek permission from the State CIO before placing wireless nodes or devices on the state's network.* State policies should also address when and how state employees may connect to the state's wired network.
- **Wireless Hot Spot Concerns:** The introduction of malicious code or other threats into the wired network has the potential to expose transmitted information and is especially a concern when state employees use public wireless hot spots to connect to the state network. To minimize these risks, both North Carolina and Michigan require wireless devices connected to the state network to have firewall and anti-virus protection. In addition, with the concerns of spyware, Michigan has included the requirement of anti-spyware software on wireless devices connecting to the state's network. However, North Carolina notes that certain

wireless devices, such as some PDAs and RFID tags, may not have those capabilities. Michigan further provides that wireless devices should only have one network interface active at any given time.

- **Other Technical Methods of Securing Wireless Connections to the Wired Network:** Device and user authentication along with a VPN are viable ways to ensure that unauthorized parties do not gain access to the wired network and the sensitive information that may be transmitted over it. For example, Michigan requires a minimum of two-factor authentication for wireless LANs, Personal Area Networks (PANs) or other types of wireless networks that are connected to the state network.
- **Restricting Access to the State Network:** *In some instances, it may be best to restrict wireless access to the state's wired network.* Due to these concerns, Washington State prohibits the use of devices connected to the state network that are also connected to an external network. Moreover, North Carolina requires that access points be segmented from an agency's internal wired LAN by using a gateway device. Finally, some activities may be restricted, such as prohibiting the management of wired IT systems by wireless devices except in cases of emergency.

A Cautionary Word about Small Wireless Devices:

Exposure of the wired network can occur via the use of small, wireless devices that are easily portable and can be used to intentionally steal information from other devices. To ensure that small wireless devices with substantial memory capabilities are not used to extract information from office computer systems, states should consider:

- **Limiting Devices Permitted in the Office:** If information stored on office computer systems or the state network is particularly sensitive, states may consider limiting the types of wireless devices that are permitted in their offices.
- **Immediate Deactivation:** *The immediate deactivation of state-issued wireless devices with memory capabilities should be mandatory prior to the actual notice of termination to an employee. This will ensure that the device is not used to compromise sensitive information transmitted by the state network or stored on fixed office computers.* In the case of an employee's resignation, devices should be immediately deactivated upon notice of the resignation. North Carolina provides for deactivation if an employee's job status changes, including a change in job function.

Recommendations for Emerging Wireless Technology Risks:

Overview of the Risk: While wireless laptops and PDAs may be common in the state workplace, other wireless technologies, such as Radio Frequency Identification (RFID) and geo-location technology, are just now emerging in the states. Potential applications include vehicle telematics using geo-location to track government or emergency vehicles for improved navigation and efficiency and RFID tags in employee ID cards for access control and/or employee time reporting.

Privacy concerns with these technologies center upon whether they are being used in a way that could be considered invasive either to citizens or state employees. For example, there are a range of concerns with tracking via geo-location and RFID technologies. The consequences can

range from the perceived erosion of individuals' anonymity to revealing other personal information by inference (for example, if a person visits a specific type of doctor's office, one might infer personal medical information) to allowing a stalker or other person with malicious intent to locate a victim and cause serious harm. Privacy advocates and others have also raised concerns that location and other information may be collected via these technologies over time, then related to specific individuals and translated into profiles of individuals' whereabouts, tastes and preferences. The following recommendations may be helpful in ensuring that new geo-location or RFID applications provide the intended benefits without creating privacy risks.

Wireless Privacy Risk Scenario #5: Can the state successfully protect any reasonable expectations of employee privacy while implementing a "contactless" employee ID card with the purpose of securing agency offices from unauthorized individuals and facilitating employee access?

A Solution: The state should conduct a privacy impact assessment to identify any ways in which the new ID cards may be invasive to reasonable employee privacy expectations. In this case, the state should determine whether the card will be used only for access control or whether information collected each time an employee swipes his or her card will be cross-matched with employee time reporting information. Any secondary uses of that data for analytics or data mining programs should be identified. In keeping with its wireless policy requirements, the state should then provide a clear explanation to employees about how the technology will be used, whether the information collected each time an employee swipes his or her ID will be combined with other information, and how long it will be stored. If information from the ID cards will be collected and stored, proper database protections should also be in place.

Recommendations:

- **Develop a Policy:** States should develop policies that address when and how geo-location technologies or RFID may be used within the state government context.
- **Conduct a Privacy Impact Assessment:** When considering a new wireless technology with geo-location or RFID, a state should conduct a privacy impact assessment to determine the nature and likelihood of any risks to individuals' location information that may be collected and/or stored.
- **Notifying Employees:** If a location-enabled technology, such as a smart phone, is issued by the state, agencies should notify individuals of the location capability, even if the state will not use it to track or otherwise locate an individual. This is similar to the state's notification to employees of the possibility of monitoring email or Internet activity. If the impacted employees are part of a labor union, the state may consider notifying the labor union as well.
- **Database Protections:** States also should ensure that proper database protections are in place for any location information that is stored in state information systems.
- **A General Note on Individuals' Personal Wireless Devices:** On a personal level, individuals should be aware of whether their personal wireless devices include location capabilities, whether those capabilities are engaged, and whether their wireless carrier maintains location information after their wireless subscription has ended.
- **General Profiling Considerations:** While profiling concerns may focus somewhat on businesses' use of geo-location and RFID-tag information, states still must be aware that

these types of emerging technologies warrant a careful examination from an employee perspective. States should consider whether the collected information will be retained, compiled or aggregated with other data, including with other personal information, and/or used for secondary purposes. Again, a privacy impact assessment early-on can be helpful.

- **Avoiding Function Creep:** States should properly scope the use of geo-location and RFID applications to avoid "function creep" regarding the secondary use of collected information. Multiple secondary uses of location or RFID tag information creates the potential for raising privacy and government profile-building concerns. For example, states should narrowly scope the use of information gained from the placement of RFID tags on license plates.
- **Have a Strategy in Mind:** If information collected from location or RFID technologies will be used in a way that could be seen by citizens as government profile-building, a state should have in place a clear strategy for addressing those concerns. State strategies should include being transparent about how that information is colleted, used, stored and/or disposed of. For example, with RFID implementations for toll road payment systems, states may consider allowing citizens to opt-out of RFID tags and providing a lane where citizens can pay with cash.

Conclusion

Our society is increasingly mobile. Wireless technologies, such as PDAs, now provide computing power, Internet access and other applications for those "on the go" and are commonplace both in the public and private sectors. Other types of wireless technologies, such as RFID and geo-location-enabled smart phones, are only now emerging in the state government and can provide location information or be used for tracking purposes. However, all of these technologies hold the potential to create exposure risks regarding the masses of sensitive information that states possess. *States must be proactive in developing privacy and security policy requirements that address wireless technology's potential risks regarding the unauthorized exposure of sensitive information. They also should address the use of wireless in ways that appear invasive to citizen privacy. With privacy concerns minimized, citizens and state employees will benefit from wireless technology without risking their privacy to do so.*

What CIOs Need to Know

- **The Role of the State CIO:** The State CIOs can serve as leaders and educators with respect to wireless technologies. In that role, they can maximize the benefits of those technologies, while minimizing the risks.
- **Adopt Enterprise Wireless Policy Provisions:** In light of the commonplace use of WLANs and portable wireless devices, the implementation of wireless security and privacy policy provisions as part of the state's overall IT security policy should be just as commonplace. *The State CIOs can serve as policy leaders to ensure that the proper policies are in place to protect sensitive information transmitted by or stored on wireless devices.* As part of data classification activities, state wireless policy provisions should identify and then protect from unauthorized exposure the types of sensitive information that are appropriate for transmission by and storage on wireless networks and devices.
- **The Risk Equation:** Given the immaturity, security weaknesses and privacy concerns related to wireless technologies, states must carefully weigh the risks and benefits of deploying such technologies. Privacy impact assessments can be a helpful tool, and the State

CIO can provide valuable insight in this analysis. In light of the risk level of some wireless technologies and the cost of countermeasures to ensure adequate privacy protections, state agencies may choose to allow these technologies to mature before deploying them. This may be particularly true for mission-critical systems where wireless technology would not contribute substantial additional benefits.

- **Matching Employee Needs to the Technology:** Minimize potential privacy exposures by matching the mobile technology device to the type of work the employee is assigned. For example, some employees, such as those in managerial positions, are message-oriented and only need email and calendar access. Others, such as field inspectors, need more robust network coverage and mobile access to online databases to complete forms in the field.
- **Acceptable Use and Training:** State wireless policies should address the acceptable uses of those technologies by state employees. They also should address employees' use of their personal devices for business purposes, wireless hot spots, and safety measures for remote wireless connections to the state's network. Employees should be required to report lost or stolen devices. Acceptable use and security awareness training on those policies can help employees prevent privacy breaches. *The state should train IT contractors in this same way.*
- **Analyze Risks Posed to the State's Wired Networks:** States should analyze the design of their wired networks in order to identify any vulnerabilities that could be exploited by wireless technologies. Small portable wireless devices can endanger the state network (and the sensitive information transmitted on it) through unsecured remote connections. Those devices can also be used in state offices to surreptitiously steal information from the network. *States may consider whether some classes of small portable wireless devices should be prohibited from use in the state workplace if the risk to sensitive information on state computers or networks is great enough.*
- **Use IT Security Controls:** IT security controls, such as firewalls, anti-virus and anti-spyware protection, encryption, VPNs, and authentication, are integral to protecting wireless technologies from breaches that could expose sensitive information.
- **Deactivation and Disposal:** To protect sensitive information stored on lost or stolen wireless devices, those devices should be enabled with remote deactivation features. States should also ensure that there are proper disposal and surplus procedures in place to avoid the retention of sensitive information on disposed or surplused wireless devices.
- **Periodic Audits:** Periodic audits will help to ensure that agencies are in full compliance with state wireless requirements. *It only takes one agency to compromise citizens' information.*
- **Know Where Your Wireless Assets Are:** Require agencies to periodically inventory and account for their wireless assets in order to identify missing or lost devices.
- **Emerging Wireless Technologies:** While wireless geo-location and RFID applications may only be emerging in the states, the State CIO can provide guidance on assessing the potential privacy impacts of these technologies early-on and should have a strategy in place for addressing privacy concerns.
- **Educate and Engage the IT Vendor Community:** States should work to educate their IT vendors to help ensure that purchased wireless technologies facilitate their wireless policies and protect citizen information. Well-educated vendors can then help inform other vendors and state agencies about the importance of wireless privacy and security.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Appendix A: Additional References and Resources

"Wireless Network Security: 802.11, BlueTooth and Handheld Devices," National Institute of Standards and Technology (NIST), Special Publication 800-48, (November 2002), <http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf>.

"From E-Government to M-Government? Emerging Practices in the Use of Mobile Technology by State Governments," IBM Center for The Business of Government, M. Jae Moon (November 2004), <http://www.businessofgovernment.org/main/publications/grant_reports/details/index.asp?gid=165>.

"M-Government: The Convergence of Wireless Technologies and E-Government," National Electronic Commerce Coordinating Council (NECCC) (2001), <http://www.ec3.org/Downloads/2001/m-Government_ED.pdf>.

"Securing Wireless Networks," Cyber Security Tip ST05-003, United States Computer Emergency Readiness Team (U.S.-CERT), (2005), <http://www.us-cert.gov/cas/tips/ST05-003.html>.

"Wireless in the Workplace: A Guide for Government Enterprises," NASCIO, (April 2004), <https://www.nascio.org/publications/index.cfm#Wireless2004>.

"Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks," GAO-05-383, Government Accountability Office (GAO), (May 2005), <http://www.gao.gov/highlights/d05383high.pdf>.

"Wireless Privacy and Spam: Issues for Congress," Marcia S. Smith, Congressional Research Service (CRS), Library of Congress, (January 26, 2005), <http://www.ipmall.info/hosted_resources/crs/RL31636_050126.pdf>.

Hearings on Wireless 411 Privacy Act, Committee on Commerce, Science and Transportation, (Sept. 21, 2004), <http://commerce.senate.gov/hearings/witnesslist.cfm?id=1315>.

An Examination of Wireless Directory Assistance Policies and Programs, U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, (September 29, 2004), <http://energycommerce.house.gov/108/Hearings/09292004hearing1387/hearing.htm>.

"Code of Conduct for Mobile Marketing," Mobile Marketing Association (MMA), (November 3, 2003), <http://www.mmaglobal.com/modules/content/index.php?id=5&submenu=conduct>.

"TrustE Security Guidelines, 1.1," TrustE, (May 2005), <http://www.truste.org/pdf/SecurityGuidelines.pdf>.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

"Wireless Security IEEE 802.11 Communications Policy," North Carolina Office of the Governor, State Chief Information Officer, (February 2005), <http://www.scio.state.nc.us/documents/docs_Active/Security%20Policies/Wireless%20Security%20IEEE%20802.11%20Communications.pdf>.

"Information Technology Security Standards," Washington State Department of Information Services, Policy No. 401-S2, (March 2005), <http://isb.wa.gov/policies/portfolio/401S.doc>.

"Policy on Infrastructure: Wireless; WLANs, WDCN, Security," Policy 1420.00, State of Michigan, (December 2002), <http://www.michigan.gov/documents/Policy_1420_59123_7.pdf>.

Locator Technologies:

"2005 Legislation Related to Event Data Recorders ("Black Boxes") in Vehicles," National Conference of State Legislatures (NCSL), (2005), <http://www.ncsl.org/programs/lis/privacy/blackbox05.htm>.

"Privacy Issues in Location-Aware Mobile Devices," Dr. Robert P. Minch, Department of Networking, Operations and Information Systems, College of Business and Economics, Boise State University, (2004), <http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650127b.pdf>.

"Web Services Applications Brief: Liberty Alliance ID-SIS Geo-Location," Liberty Alliance Project, <http://www.projectliberty.org/resources/whitepapers/IDSIS_Geo_Location.pdf>.

RFID:

"Position Statement on the Use of RFID on Consumer Products," Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC), Junkbusters, Meyda Online, and Privacy Activism, (November 2003), <http://www.privacyrights.org/ar/RFIDposition.htm>.

"RFID Radio Frequency Identification: Applications and Implications for Consumers," Federal Trade Commission (FTC), (March 2005), <http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.>.

"Information Security: Radio Frequency Identification Technology in the Federal Government," U.S. General Accountability Office (GAO), (May 2005), <http://www.gao.gov/new.items/d05551.pdf>.

"Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security and the Consumer," U.S. House of Representatives, Committee on Energy and Commerce, (July 2004), <http://energycommerce.house.gov/108/Hearings/07142004hearing1337/hearing.htm>.

"Guidelines for EPC on Consumer Products," EPCGlobal, (2005), <http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html>.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

"Radio Frequency Identification Technologies: A Workshop Summary," National Research Council, Committee on RFID Technologies, (2004), <http://www.nap.edu/catalog/11189.html>.

"2005 Privacy Legislation Related to Radio Frequency Identification (RFID)," National Conference of State Legislatures (NCSL), (2005), <http://www.ncsl.org/programs/lis/privacy/rfid05.htm>.

"Radio Frequency Identification: RFID Coming of Age," Information Technology Association of America (ITAA), (June 2004), <http://www.itaa.org/rfid/docs/rfid.pdf>.

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Appendix B: Elements for Consideration in State Wireless Policies

To properly address the privacy (and security) concerns of wireless technologies, states should consider the adoption of wireless security policy provisions as part of the state's overall IT security policy and standards. The following are elements that states may examine for possible inclusion to specifically address wireless privacy policy provisions. It is important for states to provide training to employees on the proper use of wireless technologies.

General Policy Elements:

- Specification of the types of technologies that are included in the policy
- Guidance for when and how to conduct privacy risk assessments with the introduction of a new wireless technology or information system
- General data classification categories and guidance on how to classify information
- Types of information that may be transmitted via wireless networks and devices
- Types of information that may be stored on wireless networks and devices and how long any such information may be stored
- Whether and when encryption and other protective measures should be used to protect sensitive information transmitted by or stored on wireless networks or devices
- Guidance as to the proper configurations and technical measures that agencies should use for wireless technologies
- Guidance for when and how to conduct employee security awareness training
- Requirements for the periodic inventorying of state wireless assets

Policy Guidance for Securing Wireless Access Points:

- Requirements for monitoring for rogue access points
- Guidance for the proper configuration of wireless access points
- Ensuring that Service Set Identifiers (SSID) values are changed from the manufacturer default setting and that they do not contain agency names or location identifiers

Policy Elements for Wireless Portable Devices:

- Criteria for when the state should issue a wireless portable device to a state employee
- Whether and when state employees can use their personal wireless devices for business purposes
- Acceptable use guidelines for state employees regarding their use of wireless portable devices
- Requirements for PINs and passwords to access wireless portable devices
- Guidance for reporting lost or stolen devices
- Whether and when state-issued portable wireless devices can use public wireless hot spots to connect to the state's network and what types of protective measures, including device and/or user authentication, should be used for connections through wireless public hot spots
- Requirements for the proper disposal of wireless portable devices

Use of Location or "Tracking" Technologies with Respect to State Employees:

- When and how notice of the use of such technologies should be given to state employees
- When and how such technologies may be used by the state

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org

Appendix C: Tips from US Cert on Securing Wireless Technologies

These are tips from the U.S. Computer Emergency Readiness Team (US-CERT) on what you can do to minimize risks to your wireless networks. You can view the entire US-CERT publication at: http://www.us-cert.gov/cas/tips/ST05-003.html.

- **Change default passwords** - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the device (see Choosing and Protecting Passwords for more information).
- **Restrict access** - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.
- **Encrypt the data on your network** - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data would prevent anyone who might be able to access your network from viewing your data (see Understanding Encryption for more information).
- **Protect your SSID** - To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.
- **Install a firewall** - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for more information).
- **Maintain anti-virus software** - You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up to date (see Understanding Anti-Virus Software for more information). Many of these programs also have additional features that may protect against or detect spyware and Trojan horses (see Recognizing and Avoiding Spyware and Why is Cyber Security a Problem? for more information).

201 East Main St., Suite 1405 · Lexington, KY 40507
P: (859) 514-9153 · **F:** (859) 514-9166 · **E:** nascio@amrms.com · http://www.nascio.org