NASCIO Representing Chief Information Officers of the States

Research Brief

May 2005

TLK2UL8R: The Privacy Implications of Instant and Text Messaging Technologies in State Government

Section I: Overview

Overview of the Privacy Implications of IM in State Government:

R U at Risk? Sarah, an employee for the state internal revenue agency engages in IM communications with her friend, Emily, located across town via her consumer-grade IM application. She continues the IM communication as she does her work. Suddenly, she runs across the completed tax form of Sally, another friend of hers, and is surprised that Sally is bringing in a substantial amount of income. Since Emily knows Sally too, Sarah sends the following IM communication to Emily: "U won't believe what Sally's income was last year. If I made that much, I'd be driving a BMW!"

This is an example of how personal information may find its way into IM communications in the state government context. This Brief addresses the privacy issues that can be associated with states' use of IM technology, which can have many benefits, including the quicker handling of time-sensitive communications.

Available since the early 1990s, Instant Messaging (IM) is a way for users to communicate in real-time with other IM users online via text messages. According to a recent study, more than 4 out of 10 online Americans use IM. Younger generations are more likely to use IM. For example, an estimated 46% of the Gen-Y age group (18-27 year-olds) use IM, while that number decreases to 18% for the Gen-X age group (28-39 year-olds). Twenty-one percent of IM users engage in IM communications at work.[1] In fact, wireless email devices are expected to increasingly offer IM capabilities. Consumers' growing use of IM has acted as a catalyst for the introduction of IM into state government. While IM can improve employee communications, it raises questions similar to email in terms of: (1) maintaining the privacy of citizens' personal information contained in IM communications, (2) addressing the management and retention requirements that may be necessary under public records or open meetings laws, and (3) ensuring that the IM communications are reasonably secure and do not compromise the

[1] "How Americans Use Instant Messaging: 53 million adults trade instant messages and 24% of them swap IMs more frequently than email. IM also gains a following in U.S. workplaces," Pew Internet & American Life Project, September 1, 2004, <http://www.pewinternet.org/pdfs/PIP_Instantmessage_Report.pdf>.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

state's network. This Brief will address the privacy considerations that states must address when implementing IM solutions.

Outline of the Brief: This Brief contains the following sections:

- **Section II:** What is IM? The Business Drivers and Security Concerns
- **Section III:** The Privacy Implications of IM in the State Government Context
- **Section IV:** What RU Doing? Examples of State Government and Private Sector Uses of IM
- **Section V:** Conclusion—RU 4Warned?
- **What CIOs Need to Know:** Salient Points for State CIOs
- **Appendix A:** Additional Resources
- **Appendix B:** US-CERT IM and Chat Room Safety Tips
- **Appendix C:** A Note on Chat Technology and Privacy.

A Note on Text Messaging: Mobile devices, such as cell phones and PDAs, also can be used to transmit short text messages between users. Text messaging appears to be a rapidly growing phenomenon with 25 billion text messages sent last year alone. This number is predicted to be as high as 45 billion for this year.[2] ***With the ever-increasing use of mobile technology within state government, state technology leaders should be aware that text message-enabled phones can present benefits and concerns that are similar to those associated with IM.*** States should follow the guidance for IM set out in this Brief in dealing with similar text messaging issues. However, where text messaging presents unique concerns, they are noted as such.

Section II: What is IM? The Business Drivers and Security Concerns

What is IM? IM is similar to email in that it is a text communication. However, IM's distinguishing feature is that it has the immediacy of a phone call. In order to start text-messaging, a user must obtain a subscription from an IM provider and install the client software on his or her computer. For consumers, this process can be quick, cheap and easy. An IM user communicates using real-time online conversation protocol with other IM users who are online and have their IM service engaged at that same time. Another distinguishing feature from email is that IM can involve multiple users simultaneously. Since IM is a "presence" technology, it also has the ability to allow users to know who else is online. For example, if a user has a "buddy list," then, when the user logs onto the IM service, he or she can see which people on his or her buddy list are online, too. With email, there is no way of knowing whether another person is monitoring his or her email, unless that person sends an email. IM also can be used for file-sharing and games, which has likely contributed to IM's growing popularity. Within the state government context, IM services can be used by state employees to communicate externally to others, such as contractors or family members, or internally with fellow employees.

[2] "Exploding growth in mobile messaging," Eric J. Sinrod, USA Today, January 12, 2005, <http://www.usatoday.com/tech/columnist/ericjsinrod/2005-01-12-sinrod_x.htm>.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

There are two main types of IM services available:

- **Consumer-Grade IM:** This includes the IM services offered by AOL, Yahoo and MSN. Citizens typically use consumer-grade IM for personal correspondence. These services are not interoperable with each other. This means that an AOL user cannot engage in IM communications with an MSN IM user. Moreover, a buddy list established on one consumer-grade IM service is not interoperable with a buddy list for another consumer-grade IM service. In the state workplace, such connections can be enabled to allow employees to IM others externally. The threats involved in consumer-grade IM are similar to the threats conveyed by email. For example, IM communications can transfer worms, viruses, and the like. Moreover, IM offers its own version of spam that is called "spim." Aside from these security concerns, consumer-grade IM also has concerns centering upon its lack of ability to be integrated with other consumer IM products and whether it can be scaled to accommodate large numbers of government users.
- **Enterprise-Grade IM:** These IM services are used by organizations such as corporations and states. The enterprise-grade services include client software that is located on those organizations' internal networks. These services provide enterprise users with more control over the securing of IM communications to prevent threats from being introduced into the network. Enterprise-grade IM services allow state government employees in a given agency or part of government to communicate with each other, although they cannot communicate with those outside the IM network. This can cause a problem for state employees who have a need to communicate with off-site state government contractors via IM.

The IM Business Drivers: Although it has been available since the 1990s, IM's use has increased substantially in recent years with consumers. Now, this real-time technology is migrating into the workplace, including state governments, and a recent study reflects that approximately 21% of the individuals surveyed who use IM use it at work, too. ***Gartner even predicts that, by the end of 2005, IM will surpass email as the primary way that people communicate electronically.***[3] The original thinking was that IM would not be heavily used due to the availability of email. However, IM's attractiveness in terms of its "real-time" quality and instantaneous connection to other users has increased its popularity. For consumers, it also can be relatively easy (and cheap) to acquire, install and use. Finally, with those under 30 being the most likely demographic to use IM, states are presented with a challenge in accommodating these individuals and their likely use of IM both when they are doing business with the government as citizens and working for the government as employees.

As with the introduction of other new technologies into the workplace, there have been some concerns with IM's value-add for state government employees. ***State CIOs can help determine how IM can be used in the workplace to increase productivity without compromising privacy or security.*** Some large corporate organizations have found that IM and its real-time quality can be useful in dealing with time-sensitive

[3] "Security: Instant Messaging Security Threats Doubling Every Six Months," IT Facts, March 14, 2005, <http://www.itfacts.biz/index.php?id=P2816>.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

communications.[4] In fact, a recent study predicts that, by 2008, 88% of workplace users will rely on a public IM network.[5] At the federal level, the Department of Defense, the Air Force, the Army, NIST (the National Institute for Standards and Technology), and FEMA (the Federal Emergency Management Agency) are using IM technologies. These entities are using enterprise-grade IM services that allow for real-time communications. Some of these services provide remote access for IM service users. They also can be of assistance in getting alerts to the right people and ensuring secure collaboration on time-sensitive matters.

However, as with other technologies, IM possesses the potential to provide a distraction and decrease productivity in the hands of certain users. According to a study by the Pew Internet & American Life Project, 40% of IM users at work generally use IM to communicate with co-workers. However, 33% use IM to communicate with friends and family at work. Twenty-one percent responded that they communicate via IM with both co-workers and friends and family about equally.[6] Hence, for states that permit the use of consumer-grade IM services, they must determine if and how much "incidental" IM use for communications with friends and family will be permitted. As an added layer of distraction, according to the Pew study, users of IM tend to be avid multi-taskers, having many things going at once. The IM communications just add one more facet to the multiple balls in the air that mutli-taskers routinely juggle.

Security: Security concerns, in the form of spim (IM's version of unsolicited spam emails), the transmission of viruses and worms, and malicious code scanning, appear to be increasing. In 2005 alone, there have been as many IM worms as there have been in all previous years.[7] Another study found that half of all IM users have received an unsolicited IM message from someone they do not know.[8] Security experts predict that IM may provide an attractive target for spammers and purveyors of viruses and worms as email becomes more secure and email users become savvier in dealing with security threats. IM attack vectors are deeply concerning as a growing phenomenon. The Fatso and Kelvir worms are examples that have recently exploited IM communications. In fact, Symantec estimates that IM security threats double every six months.[9]

The majority of IM threats appear to come from a contact that is known to the user. ***With the simple click of a link or download of an attachment, an infection can propagate***

[4] "Banning Instant Messaging does not reduce business risks," Continuity Central, April 28, 2004, <http://continuitycentral.com/news01168.htm>.
[5] "Instant message worm attacks increasing," Bob Sullivan, MSNBC.com, March 7, 2005, <http://www.msnbc.msn.com/id/7120241/>.
[6] "How Americans Use Instant Messaging: 53 million adults trade instant messages and 24% of them swap IMs more frequently than email. IM also gains a following in U.S. workplaces," Pew Internet & American Life Project, September 1, 2004, <http://www.pewinternet.org/pdfs/PIP_Instantmessage_Report.pdf>.
[7] "Instant message worm attacks increasing," Bob Sullivan, MSNBC.com, March 7, 2005, <http://www.msnbc.msn.com/id/7120241/>.
[8] "How Americans Use Instant Messaging: 53 million adults trade instant messages and 24% of them swap IMs more frequently than email. IM also gains a following in U.S. workplaces," Pew Internet & American Life Project, September 1, 2004, <http://www.pewinternet.org/pdfs/PIP_Instantmessage_Report.pdf>.
[9] "Security: Instant Messaging Security Threats Doubling Every Six Months," IT Facts, March 14, 2005, <http://www.itfacts.biz/index.php?id=P2816>.

Copyright © NASCIO 2005 • All rights reserved

and send itself to all of the contacts in a user's buddy list without an indication to the user of what has occurred. Attackers may even be using malicious code that attacks IM to communicate messages to one another. The good news is that hackers have not yet begun to attack IM software, likely because there are not security measures in place, as there are with email.[10] However, as the use of "smart phones"[11] with email and IM capabilities increases, so does the risk of infections spreading from PCs to smart phones via IM.

The presence of IM threats, such as spim, worms and viruses, interferes with users' perceived privacy in the same way that it interferes with email users' perceived privacy. Moreover, spim and other unwanted messages can appear when a user is in mid-conversation with another user, making the existence of these unsolicited messages all the more annoying to the user. However, there are classes of security tools on the market to counter-act security threats to IM communications.

Due to these security concerns, a best practice in the states is to block state employees' use of consumer-grade IM services in the workplace. Otherwise, these services pose risks in terms of allowing state employees to circumvent the state's security measures and the introduction of worms, viruses and the like through unsecured consumer IM services. A state can use asset management tools to determine if employees are using consumer IM services and configure state IT systems so that access to them is blocked and those IM service providers' software cannot be installed on government computers. However, if a state allows for the use of external IM services, the state should be vigilant in keeping security measures up-to-date and warning users of the danger of clicking on suspicious links. For external applications, extranet strategies or having a contractual relationship with the IM service provider can add another layer of protection.

Enterprise-grade IM services provide a good alternative to consumer-grade IM services. Since enterprise-grade IM services operate within a state's network, a state can prevent the introduction of worms, viruses and spim through IM communications. These services also provide the state with better ways to integrate IM into the state's currently-existing encryption and authentication mechanisms. Furthermore, they may include features that will log and archive communications, which can be of assistance in ensuring that IM messages comply with state IM standards and any applicable public records laws or regulations.

---

[10] "Does IM stand for insecure messaging?" Matt Hines, C|Net news.com, <http://news.com.com/Does+IM+stand+for+insecure+messaging/2100-7349_3-5629037.html?tag=nefd.lede>.

[11] A "smart phone" is "generally considered any handheld device that integrates personal information management and mobile phone capabilities in the same device. Often, this includes adding phone functions to already capable PDAs or putting "smart" capabilities, such as PDA functions, into a mobile phone. The key feature of a smart phone is that one can install additional applications to the device." For more on smart phones, please see <http://en.wikipedia.org/wiki/Smart_phone>.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

More on Text Messaging with Mobile Devices: Mobile technologies, such as text messaging-enabled cell phones, can provide an excellent way for state employees to keep up with work-related issues. However, their messaging capabilities do not have the scrutiny of the workplace due to their mobile nature. This means that text messaging from state government cell phones can provide a means for employee distraction. ***With the growth of text messaging and more employees being used to multi-tasking, states should begin dealing with the implications of cell phone and PDA text messaging now.*** Moreover, while phones are more difficult to hack into than other devices, traditional forms of security threats, including spam, viruses and worms, which are present with other types of technologies, could migrate to mobile devices.

Section III: The Privacy Implications of IM in the State Government Context

Compromising Citizens' Personal Data When Used by State Agencies for Employee Communications: If state agencies use IM, they must establish policies to address if citizens' personal information may be transmitted via IM (and, if so, under what circumstances). A state has the choice of whether to prohibit entirely the transmission of personal information via IM or to implement exceptions to this for work-related emails. However, if personal information is not permitted to be shared via IM, states should clearly tell employees that instead of relying on customary practices that may prohibit such.

Because of the similarity of IM to email (both are text messages), a state may address IM within its Acceptable Use Policy (AUP) that deals with email and Internet communications. AUPs can easily be updated with standards and guidance for whether and when state employees may use IM. ***A state may consider taking the following steps to protect the privacy of citizens' personal information in relation to IM communications:***

- ***Prohibiting the use of consumer-grade IM services in the workplace***
- ***Making guidance available on how enterprise-grade IM services can be used for IM communications, and***
- ***Determining whether citizens' personal information or other confidential communications may be included in IM communications.***

For state agencies that must comply with HIPAA's Privacy Rule and permit the use of IM, they should assess and address the use of IM and any risks that it might pose to protecting the privacy of health information under HIPAA.

Another facet of the use of IM is whether state government supervisors should monitor employees' IM communications. This determination should be guided by the state's AUP that most likely addresses whether the state can monitor employees' email and Internet use. At any rate, the state's AUP also should clearly address whether employees' IM communications are subject to monitoring.

Retention of IM Communications and Public Records and Open Meetings Laws: If a state allows employees to use IM for business purposes, the state should consider whether IM communications should be saved and maintained, like email, or whether they should be treated as voice conversations and not recorded or maintained. This difficult issue is

Copyright © NASCIO 2005 • All rights reserved

related to public records laws that may make IM communications for official business purposes subject to public disclosure. There also is the potential for IM communications among state officials to be subject to open meeting requirements if used to conduct official business that would otherwise be done in an open meeting. ***Given the potential for IM communications to constitute official communications if used for state business purposes, states should consider ways to manage and archive such communications.*** An additional consideration for states that archive IM communications is how those communications will be secured, particularly if they include personal or sensitive information.

The IM Archiving Without Consent Problem: More in the context of personal use, consumers using IM should be aware that IM applications may have an archiving function that can be engaged by the person with whom they are conversing without their knowledge. State law may or may not require that the archiving party provide the other party with notice that the conversation is being archived. Given the immediacy of IM and the potential for a consumer to perceive IM communications as informal, a consumer could have IM discussions archived without his or her knowledge or consent and later divulged to others without authorization.[12] In educating employees on the appropriate use of IM, the state also could have the opportunity to educate employees on this point for use in their personal IM communications.

Addressing Text Messaging Privacy: Text messaging generally involves privacy concerns that are similar to IM when used to conduct government business. States should consider addressing these concerns in their AUPs. They should cover the following issues:

- Whether employees can use text messaging functions on their government cell phones
- If so, whether employees' use of text messaging from their government cell phones will be limited to government business purposes
- Whether personal information can be transmitted via text messaging
- The potential impact of public records and open meetings requirements on text messaging communications
- Whether text messaging communications will be monitored by state government supervisors and, if so, whether state employees will be informed of such.

An additional concern with phones and other text messaging-enabled devices is that they can easily be lost or stolen. This could compromise any sensitive text messages stored on a user's phone or other device. Limiting the transmission of sensitive communications via text messaging and using available security measures can minimize the impact of lost or stolen mobile devices.

[12] "IM chats don't fade from PCs' memories," C|Net news.com, June 20, 2001, <http://news.com.com/2100-1023-268756.html?legacy=cnet>.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Section IV: What R U Doing? Examples of State Government and Private Sector Uses of IM

Below are examples of what some government and corporate entities are doing regarding IM services.

Examples of State IM Uses and Policies:

Arizona: This state's enterprise-wide email use policy addresses IM as part of email. Attributes of Arizona's policy include proper training before use by an employee, encryption for confidential messages, anti-virus protection, and an acknowledgment that email and IM communications are not private.

Link to Arizona's policy:
http://www.azgita.gov/policies_standards/pdf/p401%20email%20use%20policy.pdf.

Florida: The State Technology Office (STO) uses an enterprise-grade IM application that is encrypted and secured to avoid interception by unauthorized individuals, viruses and other threats. It is primarily used by STO's management.

Kentucky: The Commonwealth's AUP prohibits the use of consumer-grade IM services by state government employees. However, there are exceptions for approved, work-related matters.

Link to Kentucky's policy:
http://gotsource.ky.gov/dsweb/Get/Document-5282/CIO-60_Email_and_Internet_AUP_-_Rev_April_04.doc.

New Jersey: This state's enterprise policy on the acceptable use of the Internet also addresses IM and specifically prohibits IM for "non-work-related purposes."

Link to New Jersey's policy:
http://www.state.nj.us/it/statewide/p2iuse.htm.

North Dakota: The Information Technology Department (ITD) offers an enterprise-grade IM application to agencies in order to avoid the security and other concerns that can be associated with consumer-grade IM offerings. The state has observed that financing IM out of agencies' budgets can curb some agencies' tendencies towards the use of free consumer-grade applications as opposed to an enterprise-grade solution that involves a per-month fee. The link below includes FAQs about IM and even an IM etiquette guide for state government employees.

Link to North Dakota's State Enterprise IM Service:
http://www.state.nd.us/itd/messenger/.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Pennsylvania: The Commonwealth, through a Management Directive, prohibits the general use of IM within the enterprise network. Waivers to the directive are reviewed by the Office of Administration, Office for Information Technology. Two waivers have been granted to date in order to facilitate the working needs of individuals with disabilities, including employees, business partners or citizens. The agencies that were granted waivers use a secure IM service.

Texas: The state's Department of Information Resources (DIR) recommends that agencies should not use IM for official communications (and should publish a policy to that effect) unless an agency establishes an enterprise IM service within its organization that manages and archives IM communications.

Link to Texas' recommendation:
http://www.dir.state.tx.us/standards/srrpub04.htm.

Utah: The state uses an enterprise-grade IM application for internal communications. Consumer-grade IM applications are used on a case-by-case basis and may be used for external communications with individuals such as contractors who do not have access to the state's internal IM application.

An Example of the Federal Government's Use of IM:

FEMA's Disasterhelp.gov: FEMA (the Federal Emergency Management Agency) uses IM technology as part of its secured site for emergency management professionals. It allows those professionals to IM each other in real-time about emergency management matters.

Link to FEMA's Disasterhelp.gov: www.disasterhelp.gov.

The Use of IM within the Corporate Community:

As with government's use of IM, private sector corporations' use of IM entails balancing IM's utility with privacy, security and productivity concerns. Particularly if a corporation allows employees to use consumer-grade solutions, it is important that employees know that clicking on attachments or links contained in IM communications could download a virus and that unsecured confidential or sensitive information conveyed via IM could be intercepted by unauthorized individuals. However, corporations may choose to use an enterprise IM service.

Sample corporate usage guidelines for enterprise IM recommend the use of IM for situations such as where an employee:

- Has a quick question
- Does not want a conversation, but needs a quick answer
- Is on a phone call
- Needs to check on another person's availability
- Needs a quiet, discrete back channel of communications

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

- Has trouble with another co-worker's speech.

The inappropriate use of IM would be its use in any situation that would be inappropriate for email.

Section V: Conclusion—RU 4Warned?

Since IM technology is similar enough to email, with both technologies providing users with text-based communications, IM does not present the novel privacy and other challenges that some new technologies present. States should look to how their AUPs address email and Internet use by state employees and update them to address IM use as well.

Although many consumer-grade IM services are popular for personal correspondence, they may not be appropriate for the state government workplace. Consumer-grade IM offerings are relatively unsecure, allow for a state user to bypass the state's security measures, and generally do not come equipped with the message management and retention tools needed by states in order to ensure compliance with state open records laws. Enterprise-grade IM services address security and retention issues as well as provide more scalability and better integration into the existing state IT environment. Hence, these types of solutions may be of assistance in helping state employees preserve the privacy of any IM communications that contain citizens' personal information.

The bottom-line is that IM and text messaging are becoming more commonplace and wireless devices are becoming smarter with new communications capabilities being introduced into the marketplace. As these devices and capabilities emerge in the state government workplace, State CIOs must determine how they can be used for the benefit of the state and its citizens, while still preserving the privacy of citizens' personal information. Establishing clear policies that can be incorporated into a state's existing AUP is a way to consistently ensure that citizens' personal information remains P&C.[13]

What CIOs Need to Know

- State CIOs should consider whether IM communications will be allowed for the conducting of official state government business. IM, with its real-time quality, can be useful in dealing with time-sensitive communications. In determining how best a state can use IM services to benefit employees and raise productivity, the State CIO should examine the business need for IM versus the exposure for privacy and security breaches.
- If IM communications will be permitted, then a state should consider a management and archiving strategy for IM communications that could be considered public records. Groups of officials who use IM in conducting government business should be educated on when and how such IM use could violate open meetings laws.
- State CIOs should perform a security risk assessment to determine whether IM is placing the state's network and other IT assets at risk today.

[13] P&C is IM lingo for "private and confidential."

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

- Consumer-grade IM services are just that—they are most appropriately used by consumers for their personal correspondence outside of the workplace. When used by employees, consumer-grade IM services can simply by-pass the state's network security measures and provide a vehicle for introducing viruses, worms, and spim (IM's version of spam) into the state's IT environment. Because of this, a best practice in the states is using asset management tools to seek out state employees' use of consumer-grade IM services and configure state networks to block the further use of consumer-grade IM services.
- Enterprise-grade IM services are available and can be installed within a state's network. Such services can be more readily secured and managed by a state's IT professionals and can be more easily integrated into the state's security, authentication and other currently existing systems. Enterprise-grade IM services also focus on scalability, which can be of assistance to large or growing state organizations.
- State Acceptable Use Policies (AUPs) are an appropriate avenue to establishing if, when and how state government employees can use IM, the extent to which citizens' personal information can be transmitted via IM communications, and whether state employees' email may be subject to monitoring. This information can be incorporated into a state's existing AUP that deals with email and Internet use.
- Security solutions to protect IM can range from the elimination of public IM use by employees to a mandatory proprietary secure IM service that is offered to state employees. Solutions between these two extremes include:

  ○ Keeping IM services within the firewall
  ○ Implementing an Intrusion Detection System to detect unauthorized use
  ○ Installation of a proxy server
  ○ Filtering content for sensitive key words
  ○ Encryption of IM messages, and
  ○ Security awareness.

- Other practices to preserve the integrity of state employees' IM use may include:

  ○ Blocking file transfers and specific contractor IM products
  ○ Controlling who uses IM within the state and to whom they send IM
  ○ Activating an automatic logoff to prevent access by unauthorized individuals, and
  ○ Installing anti-virus and anti-spyware applications.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Appendix A: Additional Resources

"Using Instant Messaging and Chat Rooms Safely," United States Computer Emergency Readiness Team (US-CERT), Cyber Security Tip ST04-011: http://www.us-cert.gov/cas/tips/ST04-011.html.

"Requirements for Managing Electronic Messages as Records," ANSI/AMRA 9-2004: http://www.arma.org/bookstore/productdetail.cfm?ProductID=1499 (link to AMRA website for purchase).

IM Logics Threat Center: http://www.imlogic.com/im_threat_center/index.asp.

North Dakota's Instant Messaging Etiquette Guide: http://www.state.nd.us/itd/messenger/docs/im-etiquette.doc.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Appendix B: US-CERT IM and Chat Room Safety Tips

For more information see: http://www.us-cert.gov/cas/tips/ST04-011.html.

- **Evaluate your security settings**: Check the default settings in your software and adjust them if they are too permissive. Make sure to disable automatic downloads. Some chat software offers the ability to limit interactions to only certain users, and you may want to take advantage of these restrictions.
- **Be conscious of what information you reveal**: Be wary of revealing personal information unless you know who you are really talking to. You should also be careful about discussing anything you or your employer might consider sensitive business information over public IM or chat services (even if you are talking to someone you know in a one-to-one conversation).
- **Try to verify the identity of the person you are talking to, if it matters**: In some forums and situations, the identity of the "person" you are talking to may not matter. However, if you need to have a degree of trust in that person, either because you are sharing certain types of information or being asked to take some action like following a link or running a program, make sure the "person" you are talking to is actually that person.
- **Don't believe everything you read**: The information or advice you receive in a chat room or by IM may be false or, worse, malicious. Try to verify the information or instructions from outside sources before taking any action.
- **Keep software up-to-date**: This includes the chat software, your browser, your operating system, your mail client, and, especially, your anti-virus software.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org

Appendix C: A Note on Chat Technology and Privacy

The Technology: "Chat" technology is related to IM technology in that it allows users to talk with each other while online. This type of technology has been adopted in the state government and retail sectors for "live-help" applications that allow an Internet user to submit an inquiry to a state agency or retailer and receive back an answer in real-time. Normally, the state or retailer owns the platform for the live-help chat application or uses a platform supplied by a portal provider. The benefit of using chat technology is that it allows the live-help operators within a state government to handle multiple inquires at a time. With inquiries by phone, an operator can only process one at a time. For state live-help applications, the state is in control of the application and its users, rules and permissions. The state may use this technology to provide citizens with canned responses to common inquiries and guide citizens to webpages and documents on the state portal that they will find helpful in resolving their inquiries.

The Privacy Problem--Compromising Citizens' Personal Data When Using State Live-Help Chat Rooms: Taking into account the security measures in place, states may consider whether and what types of personal information, such as Social Security Numbers and financial account numbers, that citizens should be able to submit to the state via live-help chat services. A state may consider educating citizens via notices or other means about the types of information that are appropriate for live-help chat services (such as generalized questions about doing business with the government) and what types of information citizens should not submit due to the risks if compromised (such as SSNs). To avoid privacy and security concerns with citizens' submission of personal information in a live-help chat forum, a state may seek to implement security measures to protect that information and dispense with the need to educate citizens not to submit personal information via live-help inquiries.

Examples of State Live-Help Chats:

Utah: This state has a 24 hour a day, seven day a week chat function that is available for citizens with questions about doing business with the government. Utah was the first state to introduce the live-help chat room as a 'round the clock citizen service.

Link to Utah's 24/7 Live Help:
http://www.utah.gov/contact.html.

Virginia: The Commonwealth has a link to its live-help feature on its homepage. When clicked, the link first provides a link to the state's privacy policy and then, with another click, allows the user to begin the live-help session.

Link to Virginia's Live-Help Chat:
http://www.myvirginia.org/cmsportal/.

Copyright © NASCIO 2005 • All rights reserved
167 West Main St., Suite 600 • Lexington, KY 40507
P: (859) 514-9153 • **F:** (859) 514-9166 • **E:** nascio@amrinc.net • http://www.nascio.org