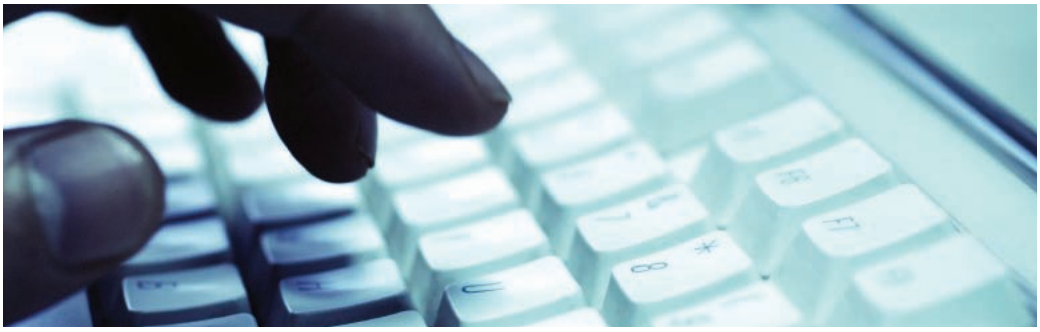
NASCIO
Representing Chief Information Officers of the States

NASCIO Staff Contact:
Mary Gay Whitmer
Senior Issues Coordinator
mwhitmer@amrms.com



The Search Is On: State CIO Starting Points for E-Discovery

Opportunities for State CIOs to Prepare for E-Discovery

NASCIO first raised e-discovery as a priority for State CIOs in its September 2007 Issue Brief entitled "Seek and Ye Shall Find? State CIOs Must Prepare Now for E-Discovery!" With new, more stringent federal rules of civil court practice requiring the production of electronic information and state courts likely to set forth similar requirements, this issue is one that necessitates State CIO involvement.[1] However, ensuring consistent and reliable mechanisms for the location and retrieval of government information across the state enterprise is a daunting task for any State CIO. Yet, e-discovery holds promise as an opportunity to leverage and pursue other State CIO priorities.

The Consolidation and Shared Services Connection: Released in August 2007, *NASCIO's Survey on Enterprise Data Center Consolidation in the States: Strategies and Business Justification* identified that there is a trend toward data center consolidation with over half of states pursuing such efforts.[2] Another recent survey, *NASCIO's Survey on IT Consolidation and Shared Services in the States: A National Assessment* found that many states are consolidating their infrastructure in order to then leverage opportunities to offer more cost-effective and efficient shared services to state agencies, such as email and data storage. Examples of such efforts are:

- Disaster recovery
- Email services
- Communications services/telephony
- ERP systems
- Networks and servers
- Portals
- Procurement
- Security services[3]

This trend towards increased consolidation and use of shared services also helps provide all agencies with access to newer technologies and increase security across the state enterprise.

In preparing for e-discovery, State CIOs can help other state government leaders realize many of these same benefits through a consistent, enterprise approach. This will allow for the creation of efficiencies and cost savings by eliminating redundant agency efforts. Cost savings also will likely be realized by the use of

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

Copyright © 2007 NASCIO
All rights reserved

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

Successfully addressing e-discovery requests entails adherence to a simple but insightful principle: Information is easier to find it if is well-organized.

records management, enterprise archiving and business intelligence tools across many agencies. Finally, security measures can be considered and implemented in a way that will ensure consistent and adequate data protection from agency-to-agency.

E-Discovery and the Electronic Records Management Opportunity: NASCIO's Enterprise Architecture Committee recently released a three-part Research Brief series entitled "Electronic Records Management and Digital Preservation—Protecting the Knowledge Assets of the State Government Enterprise" that highlights the importance of properly managing electronic government information and records as a knowledge asset.[4] A high priority CIO challenge of the day with electronic records management is how to handle "born digital" information that, from creation to destruction or permanent storage, never exists in paper form. On a broader scale, electronic records management is a necessary priority not only for CIOs but for the entire state enterprise because of the many organizational, legal and economic implications associated with it. In light of that, NASCIO has encouraged State CIOs to become advocates for improved records management of electronically-stored knowledge assets at the enterprise level and engage a variety of stakeholders, including state legal counsel, archivists, librarians, enterprise architects, records managers, and agency leaders.

Successfully addressing e-discovery requests entails adherence to a simple but insightful principle: *Information is easier to find it if is well-organized.* The organization of a state's electronic information and records is critical to the reliable and consistent fulfillment of e-discovery requests. Because of this, the need for increased organization of electronically-stored state information and records can provide the business justification for an enterprise electronic records management initiative.

The benefits of an electronic records management approach are broader than just ensuring reliable response mechanisms for e-discovery requests across the state enterprise. Liability and risk limitation, cost savings, increased consistency among agency records retention policies and practices, more thoroughly trained employees and enhanced security are just some of the additional benefits.

Background on E-Discovery and the State CIO

The E-Discovery Process: E-discovery, like many other functions that take place within government, is not just an event but is an entire process with a beginning, middle, and end. Electronic records management starts off this process and takes place before a discovery request for electronically stored information is ever made.

Once a request is submitted for information in digital form, that information must then be identified (or a determination made that it no longer exists). If the information does in fact exist, it must be located and retrieved. From there, the information most likely will be turned over to state legal counsel for review and a determination as to whether the state is legally required to produce it for the requesting party. After that, the information is produced for the requesting party or withheld on the basis of legal privilege or exception. At trial, discovery-related information may be presented if permitted according to federal or state rules of evidence.

Why State CIOs Need to Prepare for E-Discovery Requests: Recent amendments in the Federal Rules of Civil Procedure (FRCP) provide one more reason for states to better manage the information and knowledge assets that are held across the enterprise. For State CIOs, this equates to increased pressure to answer the following questions when the state is presented with a discovery request for electronic information as part of a federal lawsuit:

- Does the state have the requested information?
- If so, where is the information located?
- How can that information be retrieved?

While a state agency may be the owner of electronic information, the State CIO will likely be the official to whom legal counsel looks when that information is the subject of a discovery request.

Regardless of whether a State CIO has responsibility by statute, Executive Order or policy for electronically stored information that is potentially discoverable in litigation, the State CIO will likely be held accountable for knowing where the information is and how it can be retrieved. The State CIO also may potentially be called upon to explain why discoverable information is either missing or not retrievable in its requested form, if at all. This could be a particularly difficult situation if the state's failure to provide the required information results in sanctions, such as allowing negative inferences to be made by a jury against the state, or even in the complete loss of a critical case.

Key E-Discovery Terms: Since the e-discovery amendments arise out of the federal judiciary, a few key legal terms must be understood by State CIOs and others at the outset.

- **"Discoverable" Information:** The courts generally provide broad latitude to request information from other parties involved in a legal matter. Generally, if information is not privileged in some way and does not place an undue burden on the state to produce it (especially if it is important to a requesting party's case), then it is discoverable and the state must produce it.

- **Admissible Information:** In federal and state courts, rules of evidence govern whether the evidence, such as electronic information or even testimony from a witness, should be presented at trial. Normally, evidence that is determined to be relevant is admitted. However, many exceptions apply. For purposes of this brief, it is important to note that information does not have to be admissible in court in order to qualify as being discoverable information. The determination of admissibility at trial comes well after the determination of whether information is discoverable.

- **Public Records:** "Information" is broader than "public records"—which are generally the documents, books, papers, or other materials created or received by state agencies and/or their employees while conducting official state business. Citizens typically have the right to compel disclosure of public records via state freedom of information laws. The types of information that are determined to be official public records vary according to state law. Some states also make the distinction between records that are "public" but not subject to review via Freedom of Information Act requests and those that are considered "open public records" and hence are open for public review. Issues as to the definition and interpretation of public records laws can be very complex and subject to ongoing debate by state officials. For purposes of this brief, however, the distinction between "information" and "public records" is of particular importance. Information does not have to qualify as a public record in order to be discoverable. Thus, whether or not a record is a public record or, for that matter, an "open" public record, does not impact whether information is discoverable in a court case.

- **Electronically Stored Information (ESI):** This is intended to be a technology-neutral definition and includes, but is not limited to, electronic "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained…."[5]

- **A Legal Hold:** In the event that there is the "reasonable anticipation of litigation", parties must preserve or "hold" information that could be discoverable if litigation occurs. The purpose of a legal hold is to communicate to the appropriate individuals that the

information they have must be preserved for or in anticipation of litigation.

Getting Started on Electronic Records Management

An electronic records management initiative can reduce the risks associated with e-discovery. It is important to involve the array of interested stakeholders in managing the initiative and implementing a sound governance structure.

Creating the Electronic Records Management Team: A diverse group of stakeholders is essential to the formation of the team, because e-discovery touches a diversity of disciplines throughout state government. At a minimum, an enterprise electronic records management team should be comprised of members from the following areas:

- **Legal:** Agency legal counsel, state Attorney General, state risk management officials
- **IT:** State CIO, agency CIOs, IT security and privacy staff, and enterprise architects
- **Agency Lines of Business:** Agency leaders who own the business processes that produce the potentially discoverable information
- **Records Management:** Experts in organizing large amounts of knowledge and information assets
- **Archivists/Digital Preservation:** Experts in storing and preserving valuable state information for the long term and ensuring that it is accessible for years to come.

Looking to Enterprise Architecture as a Forum for Electronic Records Management: Enterprise Architecture (EA) is a multi-domain, multi-disciplinary forum that brings together a wide-range of state leaders to ensure that the state takes a holistic approach not only to IT and but to the way government conducts business. State EA programs can include individuals with technical backgrounds, project managers, IT security personnel, procurement, business process experts, and others. The ability of EA to convene a diversity of stakeholders to foster collaboration, shared decisions and enterprise solutions makes it an ideal home or forum for an enterprise electronic records management initiative.[6] To start such an initiative within a state's EA program, a domain team for electronic records management may be assigned with the task of examining and creating statewide standards for managing a state's electronic records.

Managing an Electronic Records Management Initiative

While efforts will vary from state-to-state, depending upon the state's needs and organizational and political structure, the maturing of a state's electronic records management processes will likely follow the general progression outlined below:

Where Is Electronic Information Located? This can be an intensive task, requiring the cooperation of agencies across the enterprise, since information can be stored in any number of state computer systems or devices, including employees' personal computers, printer and fax memory components or even in metadata.

South Dakota organizes this process by examining the devices and locations that could contain electronic information as well as examining the formats and data types in which that information may be stored.

Four Dimensions of Electronic Records:

Data Devices
Mainframes, Servers, PCs, Laptops
Cell phones, PDAs, Digital cameras
Black boxes, RFID
Thumb drives

Data Locations
In-house
Network
Hosted

Data Formats
Word processing document
Spreadsheet
Database
Email, xml, html

Digital Object Types
Office documents
Email
Databases
Webpages
Audio
Video
Voicemail
Log files
Instant Messages

Source: South Dakota Business Requirements Document for E-Mail E-Discovery and Archive Project, Bureau of Information Technology (BIT), State of South Dakota, 2007.

Who "Owns" Electronic Information? Within the lifecycle of collecting electronic information, using it, storing it, and disposing of it, state records management initiative leaders must know which agencies have physical and legal custody of the information.[7] For example, an agency may collect certain items of information electronically, such as an individual's personal information. At that point, the information is legally and physically within the agency's custody. However, that information may be stored electronically in the state's data center. During that phase, the state data center may have physical custody of the information, while the agency retains legal custody in terms of classifying the information as sensitive or personal information and keeping it according to agency records retention schedules. Moreover, when information in electronic form is collected once but shared among multiple agencies, there also can be questions about information ownership that must be sorted through as part of an electronic records management initiative.

What's Being Brought Into the State Workplace? State CIOs should keep a watchful eye on what new technologies state employees are bringing to work with them and using to store work-related information. PDAs, laptops, thumb drives and even portable digital music players can be used to store information. Additionally, consumer-grade Instant Messaging and chat technologies used at work by state employees could transmit discoverable information without a way to retain that information. In such instances, the State CIO may consider enterprise-grade solutions that provide employees with the functionality they desire while ensuring that discoverable information in electronic form is retained and retrievable.

Where Are Employees Storing Electronic Information? Employees also may attempt to store information on their desktop computers or on other media that are not regularly backed-up. Hence, states should consider requiring employees to store electronic information on shared drives that are backed-up on a regular schedule. This protects against the irreversible deletion of information and also helps to ensure that all discoverable information that is stored electronically can be found without searching many employees' desktop computer drives.

Finally, State CIOs also may be asked to evaluate new technologies that will be used by state employees in order to guard against the deletion of electronically stored information through "auto-delete" and other types of features that may be available but can be turned-off or disabled.

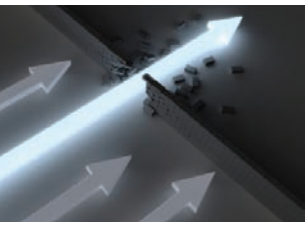
Do You See the "Hidden" Information? State CIOs may be able to contribute their technical expertise to agencies and state legal counsel regarding information that could be hidden within electronic documents and records that will be turned over to opposing counsel. This same concern applies to sensitive information, such as personal information including Social Security Numbers, that may be accidentally included when responding to a discovery request.

Today, much of the potentially discoverable electronic information may have "metadata", which is data embedded within the information that is discoverable. Metadata

State CIOs may be able to contribute their technical expertise to agencies and state legal counsel regarding information that could be hidden within electronic documents and records that will be turned over to opposing counsel.

provides "data about the data". While metadata may not be readily apparent upon viewing a document, it may yield valuable information once it is identified and analyzed. State CIOs can provide expertise about where metadata may exist and what it might say about the underlying discoverable information.

To avoid metadata or other hidden electronic information inadvertently being turned over to opposing counsel even though it may be privileged and exempt from discovery, state legal counsel may consider entering into agreements with the opposing party to deal with any such information that is turned over. An example of one type of agreement is a "claw-back" provision under which privileged information that is inadvertently turned over to opposing counsel can be taken back by a state's legal counsel.



What Are Your Priorities? Targeting the Areas of Opportunity: After analyzing where a state's electronic information is located, an important next step is prioritizing electronic information according to those types of information that may be at the most risk of not being located in response to a discovery request. Those are the types of electronic content that should be dealt with first within an electronic records management initiative to ensure that such information can be more readily located and is better organized. For many states, email may be the predominant area to target, since increasing amounts of government business and transactions are conducted via email.

How Long Do I Keep Electronic Information? The Role of Records Retention Schedules

Records retention schedules set forth the types of information that must be kept by the state, the length of time for which that information must be kept, and when it can be destroyed or purged, if ever. Schedules may be organized according to content type. These retention schedules are an integral part of the electronic records retention life cycle.[8] Each agency may have its own records retention schedule that is dictated by the type of information it collects, uses and stores and its own unique legal and business needs. However, the State CIO can play a part in ensuring that agency records retention schedules are sufficient and consistent across the state enterprise to ensure that the state does not incur liability by failing to retain discoverable electronic information.

At a minimum, state agencies should review their records retention schedules to make sure that they are up-to-date. For many states, their original records retention schedules may have been formulated and implemented when most information was collected and stored in paper form. Now, with much information being stored in electronic form and, with some of that information never existing in paper form (such documents are often referred to as "born digital"), records retention schedules may be out-dated. Moreover, with the enactment of new laws and regulations, such as those protecting the privacy of personal information, records retention schedules must take into account what electronically stored information may need to be retained for compliance purposes.

An Enterprise Approach to Records Retention Schedules—An Example from Washington State

In order to ensure compliance with e-discovery requests as well as to reduce liability for the state, Washington State took an enterprise approach that began with the creation of a cross-functional team that included the State CIO, legal counsel, business leaders, such as the Chief Financial Officer, human resources, business units, and compliance and audit. This team worked with agencies to create or update records retention policies and make them simple and easy-to-understand. Efforts focused on identifying similarities in various laws and regulations, such as e-discovery and privacy requirements, and then finding

the "high water mark" for retention timeframes.

Washington State also analyzed four approaches to retaining information for e-discovery purposes according to the relative impact of each on liability, employee productivity, process and cost. The approaches examined were:

- Save nothing
- Selective deletion
- Selective retention
- Saving more "intelligently"

Washington State opted for the last approach of saving more intelligently and focusing on a document's meaning when organizing saved information.[9]

The Importance of Using and Adhering to Records Retention Schedules: While the creation of a sound and simple records retention policy is a good first step, state agencies across the enterprise must diligently adhere to the records retention policies in order for them to be effective. This is important not only from the perspective of keeping discoverable electronic information but also destroying or purging of information that is no longer needed. The latter is concerned with electronic information that has remained in existence even though it should have been destroyed and whether that information is discoverable in litigation. This is a gray legal area that leaves the state open to liability if electronic information is not purged at the scheduled time.

A retention schedule may give an agency discretion as to whether to destroy electronic information or records after the expiration of a specific time period. In that instance, agencies should understand that extenuating circumstances such as litigation, audit, investigations and the like may necessitate retaining information longer than the specified retention period. It is important to note that purging such information once an e-discovery request has been made can make the state appear as if it is destroying electronic information according to its content and not just to adhere to records retention schedules. Liability issues aside, timely destruction and purging practices also can save the state on electronic storage and maintenance costs.[10]

In addition to records retention schedules, federal and state laws may require the retention of information for a prescribed period of time. Agency records retention schedules may reflect these legally-required retention periods. If a document is mandated to be retained by a law or regulation such as the Health Information Portability and Accountability Act (HIPAA), adherence to retention periods is particularly important. The consequences of non-compliance could be severe. For example, under the amended federal e-discovery rules, a "safe harbor" provision provides that penalties cannot be imposed for the good faith deletion of electronic information during the routine operation of an IT system. However, concerns exist that failure to comply with a legally-mandated retention requirement could be used to disqualify a party to a lawsuit from using the safe harbor provision and impose penalties for the deletion of electronic information.

The Role of Technology in Records Retention Policy Compliance: Since it can be a subjective call on the part of state employees to decide what should be saved or destroyed, State CIOs may consider automating the processes that support records retention schedules to the fullest extent possible. However, monitoring processes should be in place to ensure that utilized technologies are not subject to unacceptable failure rates.[11]

Hold It! More About Legal Holds: As pointed out earlier in the brief, if a state reasonably anticipates litigation or if litigation is pending, the state is under a duty to preserve potentially discoverable information, including that which is electronically stored. The key to this process is communicating to employees (and even contractors) their responsibility to preserve discoverable electronic information. To ensure that employees are made aware

While the creation of a sound and simple records retention policy is a good first step, state agencies across the enterprise must diligently adhere to the records retention policies in order for them to be effective.

of the legal hold procedures upfront, a state may consider requiring employees to sign an acknowledgement of legal hold procedures.

What Employees Need to Know About Legal Holds: Important items to communicate as part of the legal hold procedure include:

- Scope of the hold order and types of electronic records and any specific content covered
- Locations under hold including any employee home work stations
- Employees (and contractors) covered
- Timeframes covered[12]

States must have standard processes in place to ensure that contractors retain potentially discoverable electronic information in the same way as employees are required to do.

The Contractor Challenge: Just as employees come and go from state government, both IT and non-IT contractors also are constantly arriving to and departing from the state government enterprise. States must have standard processes in place to ensure that contractors retain potentially discoverable electronic information in the same way as employees are required to do. Incorporating provisions into contracts that address a contractor's duty to retain information created or handled by the contractor is a way to set forth record retention expectations at the beginning of a state-contractor relationship. Moreover, states may choose to have contractors sign an acknowledgment regarding record retention requirements and implement and adhere to security policies to protect information in the possession of departing contractors.

The Retrieval Challenge

E-Discovery Impact on Storage and Retrieval: Not only must electronic information be properly stored according to retention schedules but it must be stored in a way that it can be accessed and retrieved. The State of Iowa has pursued an electronic records management initiative to address the storage, access and retrieval of state information for e-discovery purposes. Iowa started with the premise that its electronic information must be brought under intellectual control, which entails documenting the origin, use, and unique record identification for each piece of information that is stored in electronic form. This includes:

- Content
- Structure (including layout and links to attachments)
- Business context (source and destination of the message and other header and property information)

As technology rapidly progresses, states may find it challenging to store electronic information in a way that can be maintained and eventually accessed and retrieved. While such information may be migrated to other hardware and software platforms in order to be preserved for the long-term, its content, structure and business context must still be preserved. State CIOs should carefully consider security measures to ensure that electronically stored information cannot be deleted, altered or otherwise manipulated over time.[13] Moreover, since states are the custodians of substantial amounts of citizens' personal information, the proper privacy policies and security measures should be in place to ensure that stored personal information is not released in an unauthorized fashion.

Tools of the Trade: If electronic information is organized in a coherent manner, then a state can be assured that it can be retrieved selectively and accurately without pulling mounds of information for state legal counsel to sort through. Tools are available for tagging electronic information to facilitate its retrieval at a later time. Search tools can provide filtering of such information by key word, business context, and even content and the meaning of documents.

The Email Storage and Retrieval Challenge: While the same electronic records management processes as outlined above apply to email, that medium presents a special challenge for states. As

state employees have become accustomed to using email to conduct business, much important state information is now stored in email form. Moreover, that may be the exclusive form of some information (meaning it was never documented on paper or in another medium). State CIOs should be aware of the following challenges that must be addressed as part of an electronic records management initiative concerning email:

- The volume of email
- The existence of multiple copies of email (sender, recipient, forwarding)
- Employees' tendency to keep everything or nothing at all
- Normalizing an email storage approach across the vast state enterprise

State Employees—The Importance of Continuing Awareness and Training Efforts

Most state employees create or handle electronic information and have at least some level of responsibility for saving or destroying that information. Given that, they must be made aware and trained on how to fulfill their specific responsibilities. One mistake, by one employee, in one agency could cost the state an important lawsuit if electronic information is either kept in violation of records retention schedules or destroyed in violation of a legal hold or retention schedules. Ongoing awareness and training activities are key, especially in the state government context that has a daily churn of new employees, resignations and terminations. One possibility for making electronic records management awareness and training uniform across the enterprise is to provide online training tools for employees, such as Michigan's online tool that educates employees on the state's records retention schedule.

Calling on the Common Threads

Inextricably intertwined, e-discovery and electronic records management issues demonstrate many principles that NASCIO has raised in previous publications including:

- **Drawing on Many Disciplines:** For any given project, multiple disciplines are likely involved. As this brief points out, electronic records management, a discipline in itself, touches many other disciplines, including security, privacy, human resources, legal, project management and more.

- **Partnership and Collaboration:** NASCIO has recognized the growing importance for State CIOs to embark upon initiatives and projects that cut across state agencies and even levels of government in two recently released Research Briefs entitled "Getting Started in Cross-Boundary Collaboration: What State CIOs Need to Know"[14] and "Connecting State and Local Government: Collaborating Through Trust and Leadership"[15]. State CIOs must work with others across the state enterprise regarding the management of the state's IT and electronically stored knowledge assets.

- **The Forum of Enterprise Architecture:** This multi-domain, multi-discipline forum is one that states may consider as a possible home for large-scale, enterprise efforts such as electronic records management initiatives, including the setting of standards for the electronic storage of information. NASCIO's Enterprise Architecture Committee has conducted much work in the discipline of electronic records management and digital preservation due to its importance to the whole of state government.[16]

- **Project Management:** The discipline of project management provides an approach that states may consider utilizing in an effort to prioritize which electronic records management issues require attention first because they present the state with the most potential risk.

- **The Role of the State CIO:** As technology continues to provide increased storage capacity and fuels the proliferation of all types of government information and data, State CIOs will be called upon to provide their expertise on how state knowledge assets can be managed in a reliable, consistent way across the whole of state government.

The Search Continues…

As states' electronic records management programs mature, State CIOs must not lose sight of the fact that electronic records management is an ongoing process pushed forward by increasing amounts of state information and new technologies to create and store such information. However, with a sound electronic records management program in place and a common understanding across the state enterprise of the importance of managing state knowledge assets, State CIOs and others who are part of the electronic records management process can meet and address those challenges that are ahead.

Appendix A: Endnotes

[1] "Seek and Ye Shall Find? State CIOs Must Prepare Now for E-Discovery!" NASCIO, September 2007, http://www.nascio.org/publications/documents/NASCIO-EDiscovery.pdf.

[2] "NASCIO's Survey on Enterprise Data Center Consolidation in the States: Strategies and Business Justification," NASCIO, August 2007, http://www.nascio.org/publications/documents/NASCIO-EnterpriseDataCenterConsolidation.pdf.

[3] "NASCIO's Survey on IT Consolidation and Shared Services in the States: A National Assessment," NASCIO, May 2006, http://www.nascio.org/publications/documents/NASCIO-ITConsolidationMay2006.pdf.

[4] "Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part I: Background, Principles, and Actions for State CIOs," NASCIO, May 2007; "Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part II: Economic, Legal and Organization Issues," NASCIO, July 2007; "Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part III: Management Leads and Technology Follows—But Collaboration is King," NASCIO, October 2007. These briefs are available at: http://www.nascio.org/publications/researchBriefs.cfm.

[5] Federal Rules of Civil Procedure, R 34

[6] "Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part I: Background, Principles, and Action for State CIOs," NASCIO, 2007.

[7] "Chief Information Officers Issue Brief: Amended Federal Rules of Civil Procedure," Iowa Information Technology Enterprise, Department of Administration, March 2007.

[8] "Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part I: Background, Principles, and Action for State CIOs," NASCIO, 2007.

[9] "Managing Legal Risk Through Records Retention and E-Mail Archiving," PowerPoint Presentation, Washington State Department of Information Services, May 2007.

[10] Ibid.

[11] "NASCIO's Electronic Records Management and Digital Preservation, Protecting the Knowledge Assets of the State Government Enterprise, Part III: Management Leads and Technology Follows—But Collaboration is King," NASCIO, October 2007, http://www.nascio.org/publications/researchBriefs.cfm.

[12] "Managing Legal Risk Through Records Retention and E-Mail Archiving," PowerPoint Presentation, Washington State Department of Information Services, May 2007.

[13] "Chief Information Officers Issue Brief: Amended Federal Rules of Civil Procedure," Iowa Information Technology Enterprise, Department of Administration, March 2007.

[14] "Getting Started in Cross-Boundary Collaboration: What State CIOs Need to Know," NASCIO, May 2007, http://www.nascio.org/publications/documents/NASCIO-CrossBoundaryCollaboration.pdf.

[15]"Connecting State and Local Government: Collaboration Through Trust and Leadership," NASCIO, November 2007, http://www.nascio.org/publications/documents/NASCIO-Cross%20BoundaryNov2007.pdf.

[16] NASCIO's Enterprise Architecture Committee Webpage, http://www.nascio.org/committees/ea/.