NASCIO
Representing Chief Information Officers of the States

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

Seek and Ye Shall Find? State CIOs Must Prepare Now for E-Discovery!

E-DISCOVERY—AN IMPACT STATEMENT FOR STATE CIOS

For Starters—What is E-Discovery?

Electronic Discovery, or "E-Discovery", is "any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case."[1] For many organizations in both the public and private sectors, preparing for e-discovery requests is likely to result in the following:

- The alteration of current business processes with respect to business records and knowledge assets
- The purchase of new technologies to manage records and knowledge assets
- An increased need to keep employees informed about their responsibilities with respect to handling records and information.

Demonstrating the impact that e-discovery will have, spending on e-discovery technologies is predicted to rise from $1.4 billion in 2006 to $4.8 billion by 2011.[2]

Why E-Discovery?

This issue is one that is quickly rising to prominence because of its significant IT, business process and operational impact on entities across the public and private sectors. As official government records and other information move into electronic form, discovery requests will be made for that information if an entity becomes involved in a lawsuit. Hence, it is critical to be able to identify where the information is located and how it can be retrieved.

Why State CIOs?

E-Discovery and State CIO Responsibilities: Prior to the commonplace use of technology to store records and other information electronically, most government records and other types of information that were created during the course of government operations were in paper form and stored in filing cabinets, shelves and archives. When discovery requests were made, pertinent documents would be turned over to legal counsel in paper form to sift through and determine what should be forwarded on to opposing counsel.

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

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

However, now, with the use of electronic documents and email to conduct state business, substantial amounts of information may never exist in paper form. Managing such "born digital" information is the issue of the day for many government organizations. Moreover, with the unprecedented increase in unstructured data, such as email, text messages and instant messages, information may be more difficult to locate and retrieve. It is within this environment that the technology expertise of the State CIO comes into play in using technology to locate electronically-stored information and successfully retrieve it when e-discovery requests are made.

Part of the State CIO's role is to ensure the proper management of information assets and not just the technological infrastructure for locating and retrieving that information.

As opposed to paper documents, the very nature of electronically stored records and information presents a number of challenges for State CIOs. For example, with paper documents, the custodian of a set of government records was easier to determine—the agency that physically held the records usually had legal responsibility for the records regarding their storage and production during discovery.

With the electronic storage of records and information, the agency that has legal responsibility for government records may not be the agency that has physical custody of them. The State CIO plays into this because the CIO may technically have physical custody over records stored in a state's consolidated data center or email system. However, the agency that created those records still may have responsibility over substantive legal questions of how to classify those records, how long they should be stored, and when, if ever, they should be destroyed or purged.

Given the blurred lines of custody regarding electronically stored records and information, questions may arise as to the State CIO's responsibility over such records. E-discovery requests for the retrieval of those records (or even a security breach with respect to those records) may point out those blurred lines of custody if they have not already been identified and clarified.

E-Discovery and the CIO Organization Business Model: State CIO organizations are often viewed as state technology service providers. In that role, the State CIO may have Service Level Agreements (SLAs) with customer agencies that detail the types of services provided to agencies and the levels at which those services will be provided. With more records and information stored electronically, the State CIO may have responsibilities regarding the storage, preservation and retrieval of those information resources.
These evolving responsibilities with respect to managing electronic records and information may require updates to currently existing SLAs. Otherwise, agencies may be functioning under incorrect assumptions regarding the State CIO's responsibility for managing electronic records, especially if they are not stored in a way that makes them easily retrievable.

Moreover, states are migrating towards greater levels of consolidation and shared services for email, data centers and other technology-related services, as identified by several NASCIO surveys of the states.[3] ***As this consolidation trend continues, State CIOs are likely to face increased questions about their responsibilities for managing state records and information housed in a consolidated environment.***

E-Discovery, Asset Management and the State CIO: From an asset management perspective, information held by a state is an asset that must be managed like any other asset. Part of the State CIO's role is to ensure the proper management of information assets and not just the technological infrastructure for locating and retrieving that information.

In the context of state government, information requested during the course of the discovery process could be located in any number of IT systems, state-issued devices or even state employees' personal IT devices, such as PDAs. In addition, potentially discoverable information must be identified as it exists within the mounds of other information held by the state and then retrieved in a form that can be

eventually handed over to the requesting legal counsel.

What's at Stake? If a state is involved in litigation, the outcome of the case could hinge upon the location and retrieval of electronic information. In the event that the State CIO cannot use the state's technology resources to locate and retrieve discoverable information, the state could be penalized to the point of turning the case to the opposing side's favor. Ultimately, a negative litigation outcome could cost substantial amounts of taxpayer dollars that might be spent on more pressing priorities.

A worst case scenario for a State CIO would be one in which the state loses a case because the State CIO was unable to find and/or retrieve requested electronic information. In such an instance, the State CIO could be placed in a position of explaining to high-level state officials, including the Governor, why the information could not be retrieved. Moreover, a State CIO might be called upon to also explain why the state's information was not organized in a locatable and retrievable fashion and why the state was unprepared for the inevitability of litigation and accompanying e-discovery requests.

Why Now? On December 1, 2006, the way that litigants in federal civil lawsuits conduct discovery changed to reflect the increasing prevalence and relevance of electronic documents and information in legal proceedings. Prior to this change, many courts had been grappling with issues surrounding the treatment of electronic records discovery. The new amendments to the Federal Rules of Civil Procedure (FRCP) in essence made it more difficult to use the fact that information is held in electronic form as a defense to fulfilling discovery requests. ***The requirement that is implicit within the new e-discovery amendments is that states must now plan ahead of time to better organize and manage their vast stores of information.***

Finally, states should also be aware of the fact that changes in the federal courts could be followed by similar changes to state court rules of civil procedure. This means that discovery requirements for state court lawsuits could also become more rigorous regarding electronic information.

A Few Starting Points

Application of the E-Discovery Amendments: The federal e-discovery amendments apply to any entity—public or private—that is involved in a lawsuit in federal court. Like any entity, the state can be involved in a proceeding in the federal court system. While states have varying levels of sovereign immunity that may be asserted as a defense to lawsuits, that fact does not prevent the filing of federal lawsuits against states. Therefore, State CIOs should anticipate the receipt of discovery requests made under the newly-amended federal e-discovery rules.

Electronically Stored Information (ESI): The e-discovery amendments refer to electronic information as ESI, or "electronically stored information". This information could be stored anywhere in the state enterprise from the state data center to an agency IT system to an employee's personal PDA that contains both personal and work-related information.

Legal Holds: States are under the duty to preserve information if they reasonably anticipate that a lawsuit may commence. In such instances, the state must issue a "legal hold" which is basically an instruction to the pertinent state employees to preserve information that could be discoverable in the eventuality that the state becomes involved in a court case.

The State CIO Impact

Equal Footing for Paper and Electronic Information: According to Ferris Research, 35% to 60% of today's critical business information is stored in email systems.[4] Moreover, roughly 97% of all information is stored electronically and as little as 3% of information is converted to paper form.[5] Given the prevalence and

potential importance of electronic information in a growing number of cases, the federal judicial system placed electronic information on the same footing as paper information via the e-discovery amendments.[6] Therefore, it is likely that e-discovery requests will become more prevalent as well and State CIOs will increasingly be faced with finding and retrieving all types of information stored electronically within the state's vast reaches.

IMPACT: To manage potential increases in discovery requests for electronic information, State CIOs must find new and innovative ways to store, organize and retrieve electronic information for the state enterprise as a whole. This may include the use of data storage systems, advanced search technologies, and business intelligence and analytical tools.

Even if information is difficult to locate, retrieve and sort through, state IT departments may be required to do so.

The Form of Electronic Information Doesn't Matter: The new e-discovery rules include within the scope of ESI information "stored in any medium" and were crafted to include all types of electronic information and incorporate future technological developments.[7]

IMPACT: Discoverable electronic information must be produced regardless of the device on which it is stored (computer, server, cell phone, PDA, digital camera, black box, RFID, thumb drive), its location (in-house, network, hosted), its format (word processing document, spreadsheet, database, email, xml, html) or digital object type (office documents, email, database, webpages, audio, video, voicemail, log files, instant messages).[8]

Production of Discoverable Electronic Information is Required: Those involved in federal cases are now specifically required to disclose electronic information at various points in time as cases proceed in the court system and can request the other side to produce such electronic information.[9] For example, as part of their mandatory initial disclosure of information supporting claims or defenses, parties to a federal lawsuit must produce electronically stored information.[10]

IMPACT: With provisions that specifically address electronically stored information, flexibility in the former version of the rules as to how to treat such information is no longer available. If electronic information qualifies as being discoverable, then it must be produced in the absence of privilege or other exception. This places added pressure on the State CIO to make sure that requested information can be found and turned over to the requesting party. In order to ensure that the state can fulfill such requests, the State CIO should be involved in planning efforts ahead of time in order to better organize and manage information held by agencies across the state.

Information in Electronic Form is No Excuse for a Failure to Produce: If electronic information is "not reasonably accessible because of undue cost or burden", then it does not have to be produced. However, the court still retains the latitude to order the discovery of such electronic information upon a showing of "good cause".[11] Judges' decisions in weighing the benefits versus the burdens of producing electronic information can be difficult. With the e-discovery amendments, no guarantees exist that difficulty in producing electronic information will constitute a sufficient excuse for non-production.

IMPACT: Even if information is difficult to locate, retrieve and sort through, state IT departments may be required to do so. The likelihood of this scenario will only increase as many documents and information will be held exclusively in electronic format. In fact, a growing amount of documentation and information is "born digital" meaning that, from the time of its creation, a document or information exists only in digital format and is never converted to a paper format.

Less Time for Finding Electronically Stored Information: At the very inception of a lawsuit, the e-discovery amendments require the production of electronic information to support each side's claims and/or defenses.[12] The rules also provide specific timeframes for production of electronic information at other points within

the course of a lawsuit. Generally, state IT departments must comply with e-discovery requests within 30 days.[13]

IMPACT: Not only do the changes in the federal rules bring with them a higher standard to meet in order to avoid production of electronic information, they also provide for tighter production timeframes in many cases. Given the complicated and large nature of some e-discovery requests, State CIOs must ensure that the appropriate business processes as well as technologies are in place to address requests as efficiently as possible and within the required timeframe.

Preservation of Electronic Information and Legal Holds: The rules recognize the difficulty of preserving electronic information due to its often voluminous and dynamic nature. The rules attempt to have states and others involved in litigation address those issues early in the discovery process, especially since the operation of most IT systems involves the automatic creation, deletion or overwriting of certain information. Decisions on what to preserve and not preserve can be difficult and involve examining the impact of preservation on the operation of critical IT systems.[14]

IMPACT: In order to identify what information must be preserved, State CIOs must ensure that the state has an adequate inventory of its IT systems, devices, applications and information. Knowing where information is located is the first step to ensuring its preservation if it could be discoverable in forthcoming or pending legal proceedings. The next step is to have the technological solutions and policies in place to preserve potentially discoverable information. To the extent possible, taking the fallible human element out of the equation through the use of technology solutions provides a sound approach to the preservation of information. For those aspects of information preservation that rely on state employees to make decisions about what information to keep, adequate training and awareness is key.

Identifying Potentially "Privileged" Information That Does Not Need to be Produced: The volume of data, its fluidity in some instances, and the existence of metadata and other "embedded" information that is not readily apparent can pose problems for asserting privilege for certain items of electronic information that may be excused from production. The amended rules recognize this and attempt to require all involved in a case to talk about these issues and reach agreements as to review protocol.[15]

IMPACT: In addition to knowing where information is located and how it can be retrieved, another important facet of e-discovery is being able to sort through substantial amounts of information in order to determine if there is information that should be withheld from discovery requests on the basis of privilege or other exceptions to the discovery rules. To the extent that technological tools can be used to accurately identify the nature and meaning of information, the risk of handing over the wrong information to the other side is lessened.

Access to IT Systems and Staff: The e-discovery amendments provide that one side may be required to grant the other side access to a specific computer or computer system as part of a discovery request. This also could include giving the requesting side technical support, information on application software or other assistance.[16] Those involved in a lawsuit also can request to "inspect, copy, test, or sample" electronic information, which could give rise to privacy and confidentiality issues that must be addressed.[17]

IMPACT: Since some cases may involve disputes as to whether electronic information is too burdensome to locate and retrieve, state IT staff may be called upon to provide depositions about how certain electronic information is stored and retrieved. In addition, parties may have the right to test or sample information from state computer systems, which creates privacy, security and logistical implications for those systems and the information within them. State IT

In order to identify what information must be preserved, State CIOs must ensure that the state has an adequate inventory of its IT systems, devices, applications and information.

staff also may be called upon to provide technical and other support in such instances. Adequate procedures and anticipating these situations can at least provide a starting point for minimizing staffing, logistical, security and privacy implications.

Lost Information Due to Routine Operation of Electronic Information Systems: The e-discovery rules implemented new provisions regarding the loss of electronic information, sanctions and penalties. This was an attempt to recognize the routine alterations and deletions of information that take place in the ordinary course of business and have nothing to do with litigation. The rules make clear that, absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.[18]

IMPACT: While sanctions may be limited when discoverable information is lost due to the routine, good faith operation of IT systems, sanctions still are possible where it appears that discoverable information has been intentionally deleted or lost. In such cases, penalties as well as rulings of inadmissibility of evidence are possible. If a state has a sufficient records management program in place, this should provide some amount of assurance to the court that the state is trying to preserve documents and other information in a good faith manner.

A Word About Contractors: State CIOs often deal with managing IT and non-IT contractors in the context of securing state IT resources that contractors may use to carryout their duties. However, State CIOs must be cognizant of managing contractors regarding the government records and information that they may handle or even create. Just because government records or information are within the physical custody of a contractor does not mean that they are exempt from coming within the state's overall approach to records management. After all, contractor records could be the subject of a discovery request. This should be factored into the IT provisions of contracts with outside service providers who may create, handle or dispose of government records or information.

The Role of Records Management and Digital Preservation in E-Discovery

Managing the volumes and volumes of various types of business information is a particularly daunting challenge for the state government enterprise. State agencies may have different IT systems, business processes, policies, records retention schedules and training practices. ***How should a State CIO proceed to ensure that electronic information is managed in a way that limits risk during e-discovery?***

An initial step is identifying the various stakeholders within state government that have a role to play and expertise to contribute regarding e-discovery. For example, the Attorney General's Office which protects the state's interest in lawsuits has an interest in being able to retrieve documents with ease and efficiency for legal purposes. Moreover, the state archivist's office has an interest in being able to store documents in a way that will make them retrievable for generations to come so that the history of the state and its operations can be preserved. Others to consider including are electronic records managers and agency CIOs, IT staff, attorneys and business managers.

Another starting point is to organize and embark on an electronic records management initiative. For example, email tends to be a very common method of communicating and conducting business. Thus, much discoverable information may be held in the form of email. Through a records management approach to email, a state can examine the gaps and shortcomings of its current email management system and develop a solution to minimize or eliminate those gaps.

Records Management and Enterprise Architecture: Taking a collaborative approach to this process is of paramount importance as pointed out in other publications of NASCIO's Enterprise Architecture Committee on records management. By drawing upon the synergy of the expertise of those with a stake in electronic records management that a state can find and implement an approach that will work for the state as an enterprise. State CIOs, records management experts, archivists and agencies must be involved and be willing to collaborate.

States also may assess how they can use the forum of Enterprise Architecture (EA) to bring together the spectrum of experts to create an electronic records management initiative that will ensure enterprise compliance with the federal e-discovery amendments. As a forum that can organize multiple domains and disciplines from across the enterprise, a state may consider EA as a proper "home" for electronic records management initiatives.[19]

The Benefits of a Collaborative Records Management Approach: This approach has many benefits including:

- Assisting all agencies through having a common, enterprise approach to the management of state records and e-discovery requests
- Reduced burden (cost and staff time) in locating and retrieving electronic information
- Increased likelihood of sound records management approaches (avoiding the two extremes of destroying everything or keeping everything)
- Ensuring that documents are destroyed according to state records retention schedules and avoiding the discovery of documents that were supposed to be destroyed according to records retention schedules but were not
- Reduction of risk and liability regarding lost electronic information
- Documenting business processes and procedures for retaining potentially discoverable information to demonstrate a state's good faith information preservation efforts
- Better trained employees regarding the management of a state's knowledge assets
- Harmonization of requirements regarding discovery of documents for state and federal litigation
- Increased ability to comply with legal and regulatory requirements, including HIPAA, Sarbanes Oxley, and the like
- Efficient and organized preservation of government documents in the state archives

Since e-discovery efforts hold promise for serving as a strong motivating force for state records management and digital preservation initiatives, NASCIO will address in a forthcoming Research Brief ways in which State CIOs can start and move forward records management and digital preservation initiatives while improving the states' ability to deal with e-discovery requests.

Appendix A: Additional Resources

NASCIO Resources:
Electronic Records Management and Digital Preservation—Protecting the Knowledge Assets of the State Government Enterprise PART I: Background, Principles, and Action for State CIOs, May 2007

New! Electronic Records Management and Digital Preservation—Protecting the Knowledge Assets of the State Government Enterprise PART II: Economic, Legal and Organizational Issues, July 2007

Forthcoming! Electronic Records Management and Digital Preservation—Protecting the Knowledge Assets of the State Government Enterprise PART III, anticipated release September 2007

See NASCIO's website for these and other resources at:
http://www.nascio.org/publications/researchBriefs.cfm.

Other Resources:
Federal Rules of Civil Procedure:
http://judiciary.house.gov/media/pdfs/printers/109th/31308.pdf

Amendment Notes to E-Discovery Provisions of the Federal Rules of Civil Procedure:
http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

- Scope of "Electronically Stored Information": Rule 34(a)
- Initial Disclosure of ESI: Rule 26(a)
- Disclosure of ESI in Interrogatories: Rules 33(d) and 34(a)
- Limitations on the Discovery of ESI for Cost or Burden: Rule 26(b)(2)(B) and (C)
- Timeframe for Responding to E-Discovery Requests: Rules 33 and 34
- Complexities of Determining if ESI is Privileged: Rule 26(f) and Notes
- Impact of E-Discovery on the Operation of IT Systems: Rule 26(f) and Notes
- Sanctions and Lost of Information Due to Routine System Operations: Rule 37(f) and Notes

Law.com's Electronic Data Discovery Webpage:
http://www.law.com/jsp/legaltechnology/edd.jsp

The Sedona Principles Addressing Electronic Document Production, 2nd Edition, The Sedona Conference, June 2007,
http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf

Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Conference of Chief Justices, August 2006,
http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf

E-Discovery and Litigation for CIOs, Executive Guide, SearchCIO.com, August 1, 2007,
http://searchcio.techtarget.com/general/0,295582,sid19_gci1266367,00.html?track=NL-274&ad=598525&asrc=EM_NLT_1911706&uid=2041789#e-discovery

Appendix B: Endnotes

[1] Searchsecurity.com definition of "e-discovery" available at: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150017,00.html.

[2] "Believe It! E-Discovery Technology Spending to Top $4.8 Billion by 2011," Forrester.com, December 11, 2006, http://www.forrester.com/Role/Research/Document/Excerpt/1,9065,40619,00.html.

[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 and "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 .

[4] "Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise PART I," May 2007, http://www.nascio.org/committees/ea/index.cfm#pubs.

[5] "Morning Coffee: Discovery Yourself," Peter Coffee, Inside EWeek Labs, October 31, 2006, citing American Bar Association statistics, http://blog.eweek.com/blogs/eweek_labs/archive/2006/10/31/MorningCoffee20061031.aspx

[6] Federal Rules of Civil Procedure: R 34(a) and Notes

[7] R 34(a) and Notes

[8] "South Dakota Business Requirements Document for Email E-Discovery and Archive Project," Bureau of Information Technology (BIT), State of South Dakota (2007).

[9] R 34(a) and R33(d)

[10] R 26(a)(1)(B)

[11] R 26(b)

[12] R 26(a)(1)(B)

[13] R 33 and 34

[14] R 26(f) and Notes

[15] Ibid.

[16] R 33(d) and Notes

[17] R 34(a) and Notes

[18] R 37(f) and Notes

[19] "NASCIO's Electronic Records Management and Digital Preservation: Protecting the Knowledge Assets of the State Government Enterprise—PARTS I and II," NASCIO, May 2007, http://www.nascio.org/committees/ea/index.cfm#pubs.